

Credit Suisse Italy S.p.A.

Modello di Organizzazione,
gestione e controllo
ex D.Lgs. 231/01

Data inizio validità: 15 Febbraio 2012
Ultimo aggiornamento: 28 aprile 2016

1 GLOSSARIO	5
2 PREMESSA.....	6
3 DECRETO LEGISLATIVO 8 GIUGNO 2001, N.231	6
3.1 Caratteristiche fondamentali ed ambito di applicazione	6
3.2 Il modello organizzativo come forma di esonero dalla responsabilità	12
3.3 L'apparato sanzionatorio	14
4 L'APPROCCIO METODOLOGICO ADOTTATO	15
4.1 La scelta di CSI	15
4.2 Il processo di redazione e implementazione ed aggiornamento del Modello 231	16
4.2.1 Approccio metodologico	16
4.2.2 Esclusione di alcuni reati non applicabili alla realtà CSI	17
4.2.3 Inclusione di ulteriori fattispecie dirette applicabili alla realtà di CSI nel corso dei Risk Assessment del 2011 e del 2015	18
4.3 Stesura del Modello 231	19
5 IL MODELLO 231	19
5.1 Finalità e struttura del modello	19
5.2 Destinatari del Modello 231	21
5.3 Adozione, modifiche e integrazioni del Modello	22
5.4 Formazione	22
6 ORGANISMO DI VIGILANZA.....	23
6.1 Identificazione dell'OdV	23
6.2 Modalità di nomina e revoca	23
6.3 Cause di ineleggibilità e motivi di revoca	24
6.4 Durata in carica dell'OdV	25
6.5 Funzioni dell'OdV	25
6.6 Obblighi di informazione verso l'Organismo di Vigilanza	27
6.7 Reporting dell'OdV	30
6.8 Conservazione delle informazioni	31
7 SISTEMA DISCIPLINARE	31
7.1 Violazioni del Modello	31
7.2 Misure nei confronti dei dipendenti	33
7.3 Violazioni del Modello 231 da parte dei dirigenti e relative misure	34
7.4 Misure nei confronti dei Consulenti, Collaboratori, Appaltatori, promotori finanziari o "Personal Banker"	35
7.5 Misure nei confronti di componenti del CdA, del collegio sindacale e dell'OdV	35
8 REATI NEI CONFRONTI DELLA PUBBLICA AMMINISTRAZIONE.....	37
8.1 Le fattispecie di reato	37
8.2 Nozione di "Pubblico Ufficiale" e "Incaricato di Pubblico Servizio"	38
8.3 Processi/Aree a rischio	40
8.4 Principi di controllo e di comportamento ed assetto del sistema di organizzazione, gestione e controllo	41
8.5 Procedure Specifiche	45
8.5.5 Sistema degli Incentivi.	48
8.6 Controlli dell'Organismo di Vigilanza	50
9 REATI SOCIETARI.....	51
9.1 Le fattispecie di reato	51
9.2 Processi/Aree a rischio e Business Unit coinvolte	53
9.3 Principi di controllo e di comportamento ed assetto del sistema di organizzazione, gestione e controllo	56
9.4 Procedure Specifiche	58
9.5 Controlli dell'Organismo di Vigilanza	67

10 REATI DI FALSITÀ IN MONETE, CARTE DI PUBBLICO CREDITO, IN VALORI DI BOLLO E IN STRUMENTI O SEGNI DI RICONOSCIMENTO.....	68
10.1 Fattispecie di reato	68
10.2 Processi/Aree a rischio	69
10.3 Principi di controllo e di comportamento ed assetto del sistema di organizzazione, gestione e controllo	70
11 REATI IN MATERIA DI INSIDER TRADING E MARKET ABUSE.....	72
11.1 Le fattispecie di reato	72
11.2 Nozione di “strumento finanziario” e “informazione privilegiata”	73
11.3 Processi/Aree a rischio	75
11.4 Principi di controllo e di comportamento ed assetto del sistema di organizzazione, gestione e controllo	76
11 PROCEDURE SPECIFICHE.....	76
11.6 Controlli dell'Organismo di Vigilanza	79
12 REATI TRANSNAZIONALI.....	81
12.1 Le Fattispecie di reato	81
12.2 Processi/Aree a rischio	82
12.3 Principi di controllo e di comportamento ed assetto del sistema di organizzazione, gestione e controllo	83
12.4 Procedure Specifiche	83
12.5 I controlli dell'Organismo di Vigilanza	84
13 REATI CON FINALITÀ DI TERRORISMO.....	85
13.1 Le fattispecie di reato	85
SI APPLICANO SIA SANZIONI AMMINISTRATIVE CHE INTERDITTIVE.....	85
13.2 Processi/Aree a rischio	86
13.3 Principi di controllo e di comportamento ed assetto del sistema di organizzazione, gestione e controllo	87
13.4 Procedure Specifiche	88
13.5 Controlli dell'Organismo di Vigilanza	88
14 DELITTI CONTRO LA PERSONALITA' INDIVIDUALE	89
14.1 Fattispecie di reato	89
14.2 Processi a Rischio	89
14.3 Principi Generali di Comportamento	89
14.4 Procedure Specifiche	89
14.5 Controlli dell'Organismo di Vigilanza	89
15 REATI IN TEMA DI SALUTE E SICUREZZA SUL LAVORO	90
15.1 Le fattispecie di reati in tema di salute e sicurezza sul lavoro	90
15.2 Processo di gestione dei rischi in materia di salute e sicurezza sul lavoro	91
15.3 Processi a Rischio	93
15.4 Principi generali di condotta e comportamento e di assetto del sistema di organizzazione, gestione e controllo	94
15.5 Principi specifici e componenti del sistema di organizzazione, gestione e controllo	94
15.6 Gestione della sicurezza per conto di altre Divisioni di CSI in Italia	99
15.7 Controlli dell'Organismo di Vigilanza	99
16 REATI DI CRIMINALITÀ INFORMATICA.....	100
16.1 Le fattispecie di reati di criminalità informatica	100
16.2 Processo di gestione della sicurezza informatica	102
16.3 Processi a Rischio	103
16.4 Principi generali di condotta e comportamento e di assetto del sistema di organizzazione, gestione e controllo	104
16.5 Procedure Specifiche	104
16.6 Controlli dell'Organismo di Vigilanza	108
17 REATI DI RICICLAGGIO.....	109

17.1 Le fattispecie di reati di ricettazione, riciclaggio, impiego di denaro, beni ed utilità di provenienza illecita e autoriciclaggio	109
17.2 Processi/Aree a rischio e BU coinvolte	111
17.3 Principi di controllo e di comportamento ed assetto del sistema di organizzazione, gestione e controllo	114
17.4 Procedure specifiche	116
I controlli dell'Organismo di Vigilanza	121
18 REATI IN MATERIA DI CRIMINALITA' ORGANIZZATA	123
18.1 La fattispecie di reato	123
18.2 Processi/Aree a Rischio	124
18.3 Principi di controllo e di comportamento ed assetto del sistema di organizzazione gestione e controllo	125
18.4 Procedure specifiche	125
19 DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO	127
19.1 La fattispecie di reato	127
19.2 Processi/aree a rischio	127
19.3 Principi di controllo e di comportamento ed assetto del sistema di organizzazione, gestione e controllo	127
19.5 I controlli dell'Organismo di Vigilanza	128
20 DELITTI IN VIOLAZIONE DEL DIRITTO DI AUTORE	129
20.1 Le fattispecie di reato	129
20.2 Principi generali di comportamento	130
20.3 Procedure specifiche	130
20.4 I controlli dell'Organismo di Vigilanza	131
21 INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA	132
21.1 La fattispecie di reato	132
21.2 Processi/Aree a rischio	137
21.3 Principi di controllo e di comportamento ed assetto del sistema di organizzazione gestione e controllo:	138
21.4 Procedure specifiche	138
21.5 I controlli dell'Organismo di Vigilanza	138
22 IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO E' IRREGOLARE	139
22.1 La fattispecie di reato	139
22.2 Processi/Aree a rischio e Business Unit coinvolte	140
22.3 Principi di controllo e di comportamento ed assetto del sistema di organizzazione, gestione e controllo	141
22.4 Procedure Specifiche	142
22.5 I controlli dell'Organismo di Vigilanza	143

1 GLOSSARIO

Appaltatori: convenzionalmente si intendono tutti gli appaltatori di opere o di servizi ai sensi del codice civile, nonché i subappaltatori, i lavoratori somministrati, i lavoratori autonomi che abbiano stipulato un contratto d'opera con CSI e di cui questa si avvale nei Processi a Rischio.

Aree a Rischio: (vedi "Processo a rischio")

Business Unit: funzione organizzativa a cui fanno capo la gestione e il governo del Processo/Area a rischio

CCNL: Contratto Collettivo Nazionale del Lavoro del settore del credito

Banca: Credit Suisse (Italy) S.p.a. iscritta all'Albo delle aziende di credito con codice ABI 3089

CdA: Consiglio d'Amministrazione

Consulenti: soggetti che agiscono in nome e/o per conto di CSI sulla base di un mandato o di un altro rapporto di collaborazione

Collaboratori: l'insieme dei lavoratori somministrati, dei lavoratori a progetto ed, in genere, dei collaboratori il cui rapporto con la Società è regolato da uno specifico contratto.

Controlli: le politiche, le prassi e le strutture organizzative disegnate per fornire ragionevoli assicurazioni in merito a:

- il raggiungimento degli obiettivi di business;
- la prevenzione dagli eventi non desiderati o la loro tempestiva rilevazione e l'adozione degli opportuni interventi correttivi.

CSI: Credit Suisse (Italy) S.p.a. iscritta all'Albo delle aziende di credito con codice ABI 3089

Decreto 231: Decreto Legislativo 8 giugno 2001, n.231

Delega: l'atto interno di attribuzione di funzioni e compiti, riflesso nel sistema di comunicazioni organizzative

Destinatari: tutti i soggetti cui è rivolto il Modello 231 e, in particolare gli organi societari ed i loro componenti, i dipendenti e i Collaboratori (ivi compresi i lavoratori somministrati, i lavoratori a progetto) e i promotori finanziari (c.d. "Personal Banker") di CSI, in quanto coinvolti nei Processi a Rischio, i Consulenti, gli Appaltatori, nonché i membri dell'Organismo di Vigilanza, in quanto non appartenenti alle categorie summenzionate

Direttive: si intendono le direttive organizzative emanate dal Gruppo e adattate alla realtà della Banca

Modello 231: insieme di norme e presidi istituiti in base al Decreto Legislativo 8 giugno 2001 n. 231, allo scopo di presidiare le Aree a Rischio

OdV: l'organismo di vigilanza la cui istituzione è prevista dal decreto legislativo 8 giugno 2001, n. 231

Operazione Sensibile: l'insieme di attività di particolare rilevanza svolte da CSI nell'ambito dei Processi a Rischio

Personal Banker: Promotori Finanziari iscritti all'albo CONSOB

Procedure: l'insieme delle disposizioni interne dirette a disciplinare l'ordinata e corretta prestazione dei servizi

Processo a Rischio: l'insieme di attività ed operazioni aziendali organizzate al fine di perseguire un determinato scopo o gestire un determinato ambito aziendale di CSI, in aree potenzialmente a rischio di commissione di uno o più reati previsti dal Decreto 231, così come elencate nella Parte Speciale del Modello 231, indicate anche genericamente e complessivamente come area/e a rischio

Process Owner: soggetto/unità/funzione organizzativa a cui fa capo la gestione e il governo del Processo a rischio

Procura: il negozio giuridico unilaterale con cui la società attribuisce dei poteri di rappresentanza nei confronti dei terzi.

2 PREMESSA

Il Modello 231 è parte integrante del "Regolamento di Direzione" di Credit Suisse Italy, documento che contiene la descrizione delle politiche di indirizzo strategico e gestionale, delle regole, delle procedure e delle istituzioni complessivamente volte ad assicurare il rispetto delle strategie aziendali, delle informazioni contabili e gestionali e la conformità delle operazioni con le disposizioni legislative e regolamentari. In particolare il "Regolamento di Direzione" (di seguito Regolamento), definisce per i dipendenti e i collaboratori, inclusi i promotori finanziari (Personal Banker), i doveri e gli obblighi da osservarsi nello svolgimento delle funzioni agli stessi assegnate.

Il suddetto Regolamento, e di conseguenza anche il presente Modello 231 in quanto parte integrante del Regolamento stesso, si inseriscono in un sistema normativo più ampio, denominato Modello Organizzativo e di Gestione, finalizzato a garantire che l'attività di Credit Suisse Italy sia svolta nel pieno rispetto delle leggi vigenti e a prevenire e sanzionare eventuali tentativi si porre in essere comportamenti a rischio

PARTE GENERALE

3 DECRETO LEGISLATIVO 8 giugno 2001, n.231

3.1 Caratteristiche fondamentali ed ambito di applicazione

Con l'entrata in vigore del Decreto Legislativo 8 giugno 2001, n. 231, recante "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica" è stata introdotta nel nostro ordinamento una responsabilità in sede penale (formalmente qualificata come responsabilità "amministrativa") degli enti.

Il legislatore italiano si è in questo modo conformato ad una serie di provvedimenti comunitari ed internazionali che richiedevano una maggiore responsabilità degli Enti che fossero coinvolti nella commissione di alcuni tipi di illeciti aventi rilevanza penale, soprattutto in materia finanziaria.

La normativa in questione prevede una responsabilità degli Enti che si aggiunge a quella delle persone fisiche che hanno materialmente realizzato l'illecito e che sorge qualora determinati reati siano commessi nell'interesse o a vantaggio dell'ente, in Italia o all'estero, da parte di:

- 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 parte di persone che esercitano anche di fatto la gestione e il controllo (i c.d. soggetti apicali);
- da persone sottoposte alla direzione o alla vigilanza di uno dei predetti soggetti apicali.

I destinatari della normativa sono ai sensi del Decreto 231: gli enti forniti di personalità giuridica e le società e associazioni anche prive di personalità giuridica. Sono espressamente sottratti all'ambito di validità del Decreto 231: lo Stato, gli enti pubblici territoriali, gli altri enti pubblici non economici, nonché gli enti che svolgono funzioni di rilievo costituzionale.

Il Decreto 231 si applica in relazione sia a reati commessi in Italia sia a quelli commessi all'estero, purché l'ente abbia nel territorio dello Stato Italiano la sede principale e nei confronti dello stesso non proceda lo Stato del luogo in cui è stato commesso il reato.

Per quel che concerne i reati per la commissione dei quali è prevista una responsabilità degli enti, il Decreto 231 prende in considerazione reati commessi nei rapporti con la Pubblica Amministrazione, i reati societari, i reati di falsità in monete, in carte di pubblico credito e in valori di bollo, i delitti commessi con finalità di terrorismo o di eversione dell'ordine democratico, i reati contro la personalità individuale, i reati di insider trading (abuso di informazioni privilegiate) e di market manipulation (manipolazione del mercato), i reati transnazionali disciplinati dalla Legge n. 146/2006, i delitti di omicidio colposo e lesioni personali colpose gravi o gravissime commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro, i delitti di riciclaggio, ricettazione ed impiego di denaro, beni o utilità di provenienza illecita, i reati informatici, i reati di criminalità organizzata, i delitti contro l'industria e il commercio ed in violazione dei diritti d'autore, i reati di falso in marchi e brevetti, il reato di induzione a non rendere o a rendere dichiarazioni mendaci all'autorità giudiziaria, nonché i reati ambientali successivamente all'approvazione in Gazzetta Ufficiale del testo del decreto legislativo approvato dal Consiglio dei ministri del 7 luglio 2011 in recepimento delle Direttive 2008/99 e 2009/123.

Più in particolare, il Decreto 231, nel suo testo originario, si riferiva esclusivamente ad una serie di reati commessi nei rapporti con la Pubblica Amministrazione, e precisamente ai reati di:

- indebita percezione di contributi, finanziamenti o altre erogazioni da parte dello Stato o di altro ente pubblico;
- malversazione a danno dello Stato o di altro ente pubblico;
- truffa in danno dello Stato o di altro ente pubblico;
- truffa aggravata per il conseguimento di erogazioni pubbliche;
- frode informatica in danno dello Stato o di altro ente pubblico;
- corruzione per un atto d'ufficio¹;
- corruzione per un atto contrario ai doveri d'ufficio;
- corruzione in atti giudiziari;
- corruzione di persona incaricata di pubblico servizio;

¹ Tale fattispecie è stata modificata dalla Legge n. 190/2012 e rubricata ora "Corruzione per l'esercizio della funzione".

- concussione, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri;
- istigazione alla corruzione;
- concussione².

Successivamente, l'art. 6 della Legge 23 novembre 2001 n. 409, recante "Disposizioni urgenti in vista dell'introduzione dell'euro", ha inserito nell'ambito del Decreto 231 l'art. 25-*bis*, che mira a punire i reati di falsità in monete, in carte di pubblico credito e in valori di bollo, ed in particolare i reati di:

- falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate;
- alterazione di monete;
- spendita e introduzione nello Stato, senza concerto, di monete falsificate;
- spendita di monete falsificate ricevute in buona fede;
- contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo;
- falsificazione dei valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati;
- uso di valori di bollo contraffatti o alterati;
- fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, valori di bollo o carta filigranata.

Successivamente, l'art. 3 del Decreto Legislativo 11 aprile 2002 n. 61, in vigore dal 16 aprile 2002, nell'ambito della riforma del diritto societario ha introdotto il nuovo art. 25-*ter* del Decreto 231, poi modificato dalla Legge 28 Dicembre 2005, n. 262, estendendo il regime di responsabilità amministrativa degli enti anche ai c.d. reati societari; più precisamente la responsabilità è stata estesa ai reati di:

- false comunicazioni sociali;
- false comunicazioni sociali in danno dei soci o dei creditori;
- falsità nelle relazioni o nelle comunicazioni della società di revisione;
- impedito controllo;
- indebita restituzione dei conferimenti;
- illegale ripartizione degli utili e delle riserve;
- illecite operazioni sulle azioni o quote sociali o della società controllante;
- operazioni in pregiudizio dei creditori;
- formazione fittizia del capitale;
- indebita ripartizione dei beni sociali da parte dei liquidatori;
- illecita influenza sull'assemblea;
- aggio;
- ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza;
- omessa comunicazione del conflitto di interessi (introdotto dalla Legge n. 262/2005).

L'art. 25 *quater*, inserito nel *corpus* originario del Decreto 231 dall'art. 3 della Legge 14 gennaio 2003, n. 7 (Ratifica della Convenzione internazionale contro il finanziamento del terrorismo), ha esteso la responsabilità amministrativa degli enti ai delitti con finalità di terrorismo e di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali e ai delitti violanti le

² Tale fattispecie è stata modificata dalla Legge n. 190/2012 con l'introduzione di un'ulteriore fattispecie di "induzione indebita a dare o promettere utilità"

prescrizioni contenute nella Convenzione summenzionata. Vengono elencati a titolo esemplificativo, ancorché non esaustivo:

- promozione, costituzione, organizzazione o direzione di associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico;
- assistenza agli associati (art. 270-ter c.p.);
- attentato per finalità terroristiche o di eversione (art. 280 c.p.);
- atto di terrorismo con ordigni micidiali o esplosivi (art. 280-bis c.p.).

L'art. 25 *quater.1*, inserito nel *corpus* originario del Decreto 231 dall'art. 3 della Legge 9 gennaio 2006, n. 7 (Disposizioni concernenti la prevenzione ed il divieto delle pratiche di mutilazione genitale femminile), ha esteso la responsabilità amministrativa degli enti al delitto di pratiche di mutilazione degli organi genitali femminili di cui all'art. 583-bis c.p..

L'art. 25 *quinquies*, inserito nel *corpus* originario del Decreto 231 dall'art. 5 della Legge 228 dell'11 agosto 2003 e modificato dalla Legge 6 febbraio 2006, n. 38 (Misure contro la tratta di persone), ha ulteriormente esteso la responsabilità amministrativa degli enti ai delitti contro la personalità individuale, quali:

- riduzione in schiavitù;
- tratta e commercio di schiavi;
- alienazione e acquisto di schiavi;
- prostituzione minorile;
- pornografia minorile;
- detenzione di materiale pornografico minorile;
- iniziative turistiche volte allo sfruttamento della prostituzione minorile.

L'art. 25 *sexies*, inserito nel *corpus* originario del Decreto 231 dall'articolo 9, comma 3 della Legge 18 aprile 2005 n. 62 (Recepimento della direttiva 2003/6/CE del Parlamento europeo e del Consiglio, del 28 gennaio 2003, relativa all'abuso di informazioni privilegiate e alla manipolazione del mercato - abusi di mercato - e delle direttive della Commissione di attuazione 2003/124/CE, 2003/125/CE e 2004/72/CE) ha ulteriormente esteso la responsabilità amministrativa degli enti ai delitti di abusi di mercato:

- abuso di informazioni privilegiate;
- manipolazione del mercato.

La medesima Legge n. 62 del 2005 ha previsto, inoltre, all'art. 187-*quinquies* Testo unico della finanza, una nuova forma di responsabilità dell'Ente conseguente alla commissione nel suo interesse o vantaggio (non di reati ma) degli illeciti amministrativi di:

- abuso di informazioni privilegiate (art. 185-*bis* Testo unico della finanza);
- manipolazione del mercato (art. 185-*ter* Testo unico della finanza).

L'art. 10 della Legge 16 marzo 2006, n. 146 - non espressamente richiamata dal Decreto 231 - come successivamente modificata, ha previsto la responsabilità amministrativa degli Enti in relazione ad una serie di reati a carattere "transnazionale" ai sensi dell'art. 3 della predetta Legge (associazione per delinquere, associazione di tipo mafioso, associazione finalizzata al traffico di sostanze stupefacenti, associazione finalizzata al contrabbando di tabacchi lavorati esteri, induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria, favoreggiamento personale, procurato ingresso illegale nel territorio dello Stato italiano o di altro Stato del quale la persona non sia cittadina e favoreggiamento della permanenza illegale).

Si considera reato transnazionale il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, 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.

Inoltre, la Legge 3 agosto 2007 n.123 ha introdotto nel Decreto 231 l'art. 25 *septies*, successivamente riformulato dall'art. 300 del D.Lgs. 9 Aprile 2008, n. 81; il suddetto art. 25 *septies* stabilisce un'ulteriore estensione della responsabilità amministrativa degli Enti in relazione ai delitti di:

- omicidio colposo commesso con violazione dell'articolo 55, comma 2, del decreto legislativo attuativo della delega di cui alla legge 3 agosto 2007, n. 123, in materia di salute e sicurezza sul lavoro;
- omicidio colposo e lesioni colpose gravi e gravissime commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

Il decreto legislativo n. 231 del 21 novembre 2007, pubblicato nel supplemento ordinario n. 268 della Gazzetta Ufficiale n. 290 del 14 Dicembre 2007, ha recepito la direttiva 2005/60/CE del Parlamento Europeo e del Consiglio del 26.10.2005, concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo (c.d. Terza direttiva Antiriciclaggio).

Tale decreto legislativo estende l'ambito di applicazione del D.Lgs. 231/2001, introducendovi l'art. 25 *octies* volto a sanzionare i delitti di:

- ricettazione (art. 648 del Codice Penale);
- riciclaggio (art. 648 *bis* del Codice Penale);
- impiego di denaro, beni o utilità di provenienza illecita (art. 648 *ter* del Codice Penale).

La Legge 18 Marzo 2008, n. 48, ha introdotto nel corpus del D.Lgs. n. 231/2001 l'art. 24 *bis*, estendendo così la responsabilità degli enti anche ai reati informatici previsti dai seguenti articoli del Codice Penale:

- 615 *ter*, (accesso abusivo ad un sistema informatico o telematico);
- 615 *quater* (detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici);
- 615 *quinquies* (diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico);
- 617 *quater* (intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche);
- 617 *quinquies*, (installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche);
- 635 *bis*, (danneggiamento di informazioni, dati e programmi informatici); 635 *ter*, (danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità);
- 635 *quater* (danneggiamento di sistemi informatici o telematici);
- 635 *quinquies*, (danneggiamento di sistemi informatici o telematici di pubblica utilità);
- 491 *bis* (falsità in un documento informatico pubblico o avente efficacia probatoria);
- 640 *quinquies* (frode informatica del certificatore di firma elettronica).

Il D.Lgs. n. 81 del 9 aprile 2008 recante "Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro", riformula l'art. 25 *septies* introdotto dalla Legge 3 agosto 2007 n.123 che estendeva la responsabilità degli enti ai delitti di omicidio colposo e lesioni colpose gravi e gravissime commesse in violazione delle norme sulla sicurezza e tutela della salute nei luoghi di lavoro.

La Legge 15 luglio 2009, n. 94, recante “Disposizioni in materia di sicurezza pubblica”, ha introdotto i reati in materia di criminalità organizzata, di cui al nuovo art. 24-ter, tra i quali l'associazione a delinquere (art. 416 c.p.) e l'associazione di tipo mafioso (art. 416 bis c.p.).

La Legge 23 luglio 2009, n. 99, recante “Disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in materia di energia” ha introdotto i reati di falso in materia di marchi e brevetti, di cui al novellato art. 25-bis (art. 473 c.p. e 474 c.p.), i reati contro l'industria ed il commercio, di cui al nuovo art. 25-bis.1 e i reati in materia di violazione della legge sul diritto d'autore, di cui al nuovo art. 25-novies.

La Legge 3 Agosto 2009, n. 166 di ratifica della Convenzione ONU sulla corruzione del 31.10.2003 ha introdotto il reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria, di cui al nuovo art. 25-decies.

Hanno in seguito avuto impatto sul *corpus* del D.Lgs. 231/2001 i seguenti provvedimenti normativi:

- D.Lgs. n. 106 del 3 agosto 2009 recante Disposizioni integrative e correttive del D.Lgs. n. 81 del 9 aprile 2008, in materia di tutela della salute e della sicurezza nei luoghi di lavoro;
- D.Lgs. n. 39 del 27 gennaio 2010 (Attuazione della direttiva 2006/43/CE, relativa alle revisioni legali dei conti annuali e dei conti consolidati) recante l'abrogazione e la modifica di reati presupposto dell'illecito amministrativo di cui all'articolo 25-ter del D.Lgs. 231/2001;
- Legge n. 96 del 4 giugno 2010 recante Disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee - Legge Comunitaria 200;

Legge n. 122 del 30 luglio 2010 recante Misure urgenti in materia di stabilizzazione finanziaria e di competitività economica;

- Legge n. 136 del 13 agosto 2010 recante Piano straordinario contro le mafie, nonché delega al governo in materia di normativa antimafia.

Successivamente, il D.lgs. 121/2011, in vigore dal 16 agosto 2011, ha introdotto nel novero dei reati di cui al Decreto anche i reati in materia ambientale (art. 25 undecies), quali:

- uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (art. 727 bis c.p.) e distruzione o deterioramento di habitat all'interno di un sito protetto (art. 733 bis c.p.);
- scarico illecito di acque reflue industriali contenenti sostanze pericolose (art. 137, D.lgs. 152/2006), gestione di rifiuti non autorizzata (art. 256, D.lgs. 152/2006) omessa bonifica dei siti (art. 257, D.lgs. 152/2006); violazioni degli obblighi di tenuta dei formulari nel trasporto di rifiuti (art. 258, D.lgs. 152/2006); traffico illecito di rifiuti (art. 259, D.lgs. 152/2006); attività organizzate per il traffico illecito di rifiuti (art. 260, D.lgs. 152/2006); violazione dei controlli sulla tracciabilità dei rifiuti (260 bis, D.lgs. 152/2006); violazione delle prescrizioni in tema di esercizio di stabilimenti (art. 279, D.lgs. 152/2006);
- commercio di animali in via di estinzione in violazione delle prescrizioni previste dalla stessa legge (art. 1 e 2 della Legge 150/1992), alla detenzione di animali selvatici che costituiscano pericolo per la salute e l'incolumità pubblica (art. 6 della Legge 150/1992); alla falsificazione e alterazione della certificazione necessaria per introdurre specie protette nella comunità europea (art. 3 bis della Legge 150/1992);
- utilizzo di sostanze lesive per l'ozono (art. 3 della legge 28 dicembre 1999, n. 549);

inquinamento doloso (art. 8, D.lgs. 202/2007) e inquinamento colposo (art. 9, D.lgs. 202/2007) dell'ambiente marino realizzato mediante lo scarico di navi.

Il D.Lgs. 16 luglio 2012, n. 109 ha introdotto nel *corpus* del Decreto l'art. 25-*duodecies*, che sanziona il delitto di impiego di cittadini di paesi terzi il cui soggiorno è irregolare, previsto dall'art. 22, comma 12-bis, D.Lgs. 25 luglio 1998, n. 286.

La Legge n. 190 del 6 novembre 2012, in vigore dal 28 novembre 2012, ha inserito all'art. 25 del Decreto il reato di "induzione indebita a dare o promettere utilità" (art. 319-quater c.p.) e all'art. 25-*ter* dello stesso il reato di corruzione tra privati (art. 2635 c.c.).

La legge n. 186 del 15 dicembre 2014, in vigore dall'1 gennaio 2015, ha inserito tra i reati presupposto richiamati dall'art. 25-*octies* del Decreto l'art. 648-ter.1 c.p., che punisce il delitto di autoriciclaggio.

La Legge 22 Maggio 2015, n. 68, entrata in vigore in data 29.05.2015, ha modificato l'art. 25-*undecies*, inserendo nei reati presupposto dello stesso nuove fattispecie di delitti ambientali (inquinamento ambientale, disastro ambientale, inquinamento ambientale e disastro ambientale commessi con colpa ai sensi dell'art. 452-quinquies c.p., delitti associativi (ovvero associazione per delinquere ed associazione di tipo mafioso) aggravati ai sensi dell'art. 452 – *octies* c.p., traffico e abbandono di materiale ad alta radioattività).

Infine, la Legge 30 Maggio 2015, n. 69, ha modificato l'art. 25-*ter* del Decreto e ha previsto alcune modifiche agli artt. 2621 e 2622 c.c.

3.2 Il modello organizzativo come forma di esonero dalla responsabilità

Il Decreto 231 prevede che l'ente non risponda dei reati commessi dai soggetti c.d. apicali qualora dimostri:

- di aver adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quelli verificatisi;
- di aver affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento;
- che le persone hanno commesso il reato eludendo fraudolentemente i suddetti modelli di organizzazione e di gestione;
- che non vi è stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.

Per i reati commessi da soggetti non in posizione apicale l'ente è responsabile solo qualora la commissione del reato sia stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza. In ogni caso è esclusa l'omissione degli obblighi di direzione e vigilanza se, prima della commissione del reato, l'ente ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi.

Il Decreto 231 prevede inoltre che i suddetti Modelli debbano rispondere alle seguenti esigenze:

- a) individuare le attività nel cui ambito esiste la possibilità che vengano commessi i reati;
- b) prevedere specifici protocolli (i.e. Direttive e Procedure) diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati da prevenire;
- c) individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- d) prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del Modello 231;

- e) introdurre un sistema disciplinare privato idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello 231.

Lo stesso Decreto 231 prevede che gli enti, per soddisfare le predette esigenze, possano adottare modelli di organizzazione e di gestione “sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti, comunicati al Ministero della Giustizia che, di concerto con i Ministeri competenti, può formulare entro trenta giorni osservazioni sulla idoneità dei modelli a prevenire i reati”.

In conformità a tale disposizione CSI, nella predisposizione della prima versione del presente Modello 231, si è ispirata alle linee guida emanate dall'ABI e da Confindustria nei rispettivi aggiornamenti al 21 maggio 2008 e al 31 marzo 2008. Nel 2011, in una successiva fase di aggiornamento, ci si è riferiti sia agli aggiornamenti emanati dall'ABI (Linee guida del 9 gennaio 2009 e del 27 gennaio 2010 relative ai reati in materia di riciclaggio e di criminalità informatica), nonché alle Linee Guida emanate nel 2010 da AIBE, Associazione delle Banche Estere in Italia.

Infine, il Modello è stato ulteriormente aggiornato nel 2015, e tale intervento si è ispirato alle Linee Guida emanate dall'ABI in data 12 luglio 2015 (in materia di reati ambientali) e alle Linee Guida di Confindustria, nella versione aggiornata al mese di Luglio 2014.

Le Linee Guida costituiscono e devono essere considerate come un semplice quadro di riferimento a cui ispirarsi nell'elaborazione del Modello, che deve invece riflettere le caratteristiche concrete della realtà, organizzazione e specifica attività dell'ente.

E' opportuno evidenziare che il mancato rispetto di punti specifici delle predette Linee Guida non inficia la validità del Modello 231. Il singolo Modello 231, infatti, dovendo essere redatto con riferimento alla realtà concreta della società, ben può discostarsi dalle Linee Guida che, per loro natura, hanno carattere generale.

Inoltre, con specifico riferimento alla materia della salute e sicurezza sul luogo di lavoro, è doveroso ricordare che l'art. 30 del D.Lgs. 9 Aprile 2008, n. 81, stabilisce che il modello di organizzazione e di gestione idoneo ad avere efficacia esimente della responsabilità amministrativa degli enti di cui al Decreto 231, deve essere adottato ed efficacemente attuato, assicurando un sistema aziendale per l'adempimento di tutti gli obblighi giuridici relativi:

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

Il suddetto modello organizzativo e gestionale deve prevedere idonei sistemi di registrazione dell'avvenuta effettuazione delle attività in precedenza elencate.

Il modello organizzativo deve altresì prevedere un idoneo sistema di controllo sull'attuazione dello stesso e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate.

Il riesame e l'eventuale modifica del modello organizzativo devono essere adottati quando:

- siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero
- in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico.

Infine, il suddetto art. 30 stabilisce che, in sede di prima applicazione, i modelli di organizzazione aziendale definiti conformemente:

- alle Linee guida UNI-INAIL per un sistema di gestione della salute e sicurezza sul lavoro (SGSL) del 28 settembre 2001, ovvero
- al British Standard OHSAS 18001:2007

si presumono conformi ai requisiti più sopra enunciati per le parti corrispondenti.

Agli stessi fini ulteriori modelli di organizzazione e gestione aziendale potranno essere indicati dalla Commissione consultiva permanente per la salute e la sicurezza sul lavoro, istituita presso il Ministero del Lavoro e della Previdenza Sociale dall'art. 6 del D.Lgs. n. 81/2008.

3.3 L'apparato sanzionatorio

Il Decreto 231 prevede che agli enti possano essere applicate sanzioni pecuniarie e sanzioni interdittive. In particolare, nel settore bancario è previsto l'intervento della Banca d'Italia sia con un ruolo di collaborazione con il pubblico ministero e con il giudice del procedimento penale, sia con l'incarico di porre in essere l'esecuzione delle eventuali sanzioni interdittive disposte nei confronti di una banca, di cui all'art. 9, comma 2, lettere a) – interdizione dall'esercizio dell'attività e b) – sospensione o revoca dall'autorizzazione.

Le sanzioni pecuniarie si applicano ogniqualevolta un ente commetta uno degli illeciti previsti dal Decreto 231, mentre quelle interdittive possono essere applicate solo in relazione ai reati per i quali sono espressamente previste dal Decreto 231, qualora ricorra almeno una delle seguenti condizioni:

- l'ente ha tratto dal reato un profitto di rilevante entità ed il reato è stato commesso
 - (i) da soggetti in posizione apicale, ovvero
 - (ii) da soggetti sottoposti all'altrui direzione e vigilanza quando la commissione del reato è stata determinata o agevolata da gravi carenze organizzative;

- in caso di reiterazione degli illeciti.

Ai fini della quantificazione delle sanzioni pecuniarie il giudice deve tenere conto:

- della gravità del fatto;
- del grado di responsabilità dell'ente;
- dell'attività svolta dall'ente per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti;
- delle condizioni economiche e patrimoniali dell'ente.

Le sanzioni interdittive applicabili agli enti ai sensi del Decreto 231 sono:

- l'interdizione dall'esercizio dell'attività;
- la sospensione o revoca di autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di pubblico servizio;
- la esclusione da agevolazioni, finanziamenti, contributi o sussidi e nella revoca di quelli già concessi;
- il divieto di pubblicizzare beni e servizi.

Il tipo e la durata delle sanzioni interdittive sono stabiliti dal giudice sulla base dei criteri indicati per la commisurazione delle sanzioni pecuniarie. Il Decreto 231 prevede, inoltre, la possibilità applicare alcune sanzioni in via definitiva (quindi superando il limite massimo di durata), qualora si verificino determinati eventi considerati particolarmente gravi.

Con specifico riferimento al settore bancario, in virtù dell'art. 97 bis, quarto comma del Testo Unico Bancario, le sanzioni interdittive di cui alle lettere a) e b) dell'art. 9, secondo comma del Decreto (interdizione dall'esercizio dell'attività e sospensione o revoca dell'autorizzazione) non possono essere applicate in via cautelare alle banche. La stessa norma stabilisce, altresì, un flusso informativo tra il Pubblico Ministero che iscrive nel registro delle notizie di reato un illecito amministrativo a carico di una banca e la Banca d'Italia e la Consob, le quali possono essere sentite nel corso del procedimento ed hanno, in ogni caso la facoltà di presentare relazioni scritte³.

Il giudice può disporre, in luogo dell'applicazione della sanzione interdittiva, la prosecuzione dell'attività dell'ente da parte di un commissario per un periodo pari alla durata della pena interdittiva che sarebbe stata applicata, qualora ricorra almeno una delle seguenti condizioni:

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

Oltre alle predette sanzioni, il Decreto 231 prevede che venga sempre disposta la confisca del prezzo o del profitto del reato, che può avvenire anche per equivalente, nonché la pubblicazione della sentenza di condanna in presenza di una sanzione interdittiva.

4 L'APPROCCIO METODOLOGICO ADOTTATO

4.1 La scelta di CSI

Nonostante il Decreto 231 consideri facoltativa l'adozione di un modello di organizzazione, gestione e controllo, CSI ha ritenuto indispensabile provvedere in tal senso poiché correttezza e trasparenza nella conduzione degli affari e delle attività di CSI sono valori espressione della politica aziendale e contribuiscono a tutelare l'immagine di CSI e le aspettative dei suoi clienti. È, dunque, interesse di CSI attivarsi in ogni modo per garantirne il rispetto.

CSI dispone già di un articolato sistema di strumenti organizzativi e di controllo (codici di condotta, policy, direttive, procedure, disposizioni organizzative, etc.) volti a tutelare i predetti valori. Tuttavia,

³ Art. 97-bis del Testo unico bancario, così come inserito dall'art. 8 del D.L.vo 9 luglio 2004, n. 197 (Responsabilità per illecito amministrativo dipendente da reato) 1. "Il pubblico ministero che iscrive, ai sensi dell'articolo 55 del decreto legislativo 8 giugno 2001, n. 231, nel registro delle notizie di reato un illecito amministrativo a carico di una banca ne dà comunicazione alla Banca d'Italia e, con riguardo ai servizi di investimento, anche alla CONSOB. Nel corso del procedimento, ove il pubblico ministero ne faccia richiesta, vengono sentite la Banca d'Italia e, per i profili di competenza, anche la CONSOB, le quali hanno, in ogni caso, facoltà di presentare relazioni scritte. 2. In ogni grado del giudizio di merito, prima della sentenza, il giudice dispone, anche d'ufficio, l'acquisizione dalla Banca d'Italia e dalla CONSOB, per i profili di specifica competenza, di aggiornate informazioni sulla situazione della banca, con particolare riguardo alla struttura organizzativa e di controllo. 3. La sentenza irrevocabile che irroga nei confronti di una banca le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a) e b), del decreto legislativo 8 giugno 2001, n. 231, decorsi i termini per la conversione delle sanzioni medesime, e' trasmessa per l'esecuzione dall'Autorità giudiziaria alla Banca d'Italia. A tale fine la Banca d'Italia può proporre o adottare gli atti previsti dal titolo IV, avendo presenti le caratteristiche della sanzione irrogata e le preminenti finalità di salvaguardia della stabilità e di tutela dei diritti dei depositanti e della clientela. 4. Le sanzioni interdittive indicate nell'articolo 9, comma 2, lettere a) e b), del decreto legislativo 8 giugno 2001, n. 231, non possono essere applicate in via cautelare alle banche. Alle medesime non si applica, altresì, l'articolo 15 del decreto legislativo 8 giugno 2001, n. 231. 5. Il presente articolo si applica, in quanto compatibile, alle succursali italiane di banche comunitarie o extracomunitarie".

per dare piena attuazione al Decreto 231, tali strumenti sono stati integrati con il Modello 231 che, per le finalità che intende perseguire, ha una portata diversa rispetto ad essi.

L'elenco di tali documenti è contenuto nel "Regolamento di Direzione CSI". In particolare, tra questi documenti, si segnalano il **Codice di Condotta** e il **Codice Etico** che definiscono i principi etici generali di condotta e che, per la loro rilevanza, sono da considerarsi parte integrante del Modello 231.

4.2 Il processo di redazione e implementazione ed aggiornamento del Modello 231

La prima versione del Modello risale al dicembre 2009, con data di validità 4 gennaio 2010.

Nel corso del 2011, il Consiglio di Amministrazione, di concerto con l'Organismo di Vigilanza, ha provveduto, avvalendosi del supporto di consulenti esterni, ad un successivo aggiornamento del Modello e, in particolare, all'integrazione della Parte Speciale con i reati di più recente introduzione, per i quali non erano state individuate, nella stesura iniziale, le aree e i processi aziendali sensibili alla commissione di tali fattispecie di reato. Nello specifico, ci si riferisce ai reati di cui agli artt.:

- 24-ter: reati in materia di criminalità organizzata,
- 25-bis: reati di falso in materia di marchi e brevetti
- 25-bis.1: reati contro l'industria ed il commercio
- 25-novies: reati in materia di violazione della legge sul diritto d'autore
- 25-decies: reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria

Infine, nel corso del 2015, a seguito dell'introduzione, nel D.Lgs. 231/2001, dei reati presupposto di impiego di cittadini di paesi terzi il cui soggiorno è irregolare (punito dall'art. 22, comma 12-bis D.Lgs. 286/1998, richiamato dall'art. 25-duodecies D.Lgs. 231/2001), corruzione tra privati (punito dall'art. 2635 c.c., richiamato dall'art. 25-ter D.Lgs. 231/2001) e autoriciclaggio (punito dall'art. 648-ter.1 c.p., richiamato dall'art. 25-octies D.Lgs. 231/2001), la Banca ha intrapreso un processo di aggiornamento dell'analisi precedentemente condotta, conseguentemente integrando ed aggiornando il proprio Modello.

Il Modello, così aggiornato ed integrato, è stato approvato dal Consiglio di Amministrazione della Banca nell'adunanza del 17 dicembre 2015.

Coerentemente con quanto previsto al punto 5.3, la revisione e l'aggiornamento del presente Modello sono rimesse alla competenza del Consiglio di Amministrazione in quanto sono apportate modifiche di carattere sostanziale, quali, nello specifico:

- integrazione della Parte Speciale con ulteriori sezioni dedicate a nuove eventuali categorie di reato applicabili alla realtà CSI;
- aggiornamento/modifica/integrazione dei principi di controllo e delle regole comportamentali.

4.2.1 Approccio metodologico

Ai fini della predisposizione del presente documento, coerentemente con le disposizioni del Decreto, con le Linee-guida Confindustria e ABI e con le indicazioni desumibili dalla giurisprudenza, la Società ha proceduto a svolgere una preventiva attività di cd. control and risk self assessment.

Le attività di control and risk self assessment sono state condotte e coordinate a cura di un Team di Progetto costituito dai consulenti esterni e hanno visto il coinvolgimento diretto del Management della Società.

In particolare, le fasi di revisione ed aggiornamento del Modello 231 di CSI sono state realizzate mediante una serie di attività qui di seguito descritte:

- **raccolta e analisi** della documentazione interna aggiornata (Organigramma, Mansionario, Regolamento di Direzione, Codice di Condotta, deleghe, procure e poteri, *global policy*, politiche e procedure operative ecc.);
- **interviste** con responsabili di funzione (soggetti apicali) e membri dell'Organismo di Vigilanza;
- **analisi del Modello vigente, revisione ed integrazione delle aree/processi a rischio** precedentemente individuate;
- **inclusione** nel Modello della descrizione analitica **delle fattispecie di reato di più recente introduzione**, non precedentemente censite ed **individuazione delle aree/processi** aziendali potenzialmente a rischio di commissione di tali reati;
- definizione, aggiornamento ed integrazione dei **principi generali di comportamento** e di **procedure specifiche** per ogni processo a rischio;
- **identificazione e valutazione complessiva del rischio** all'interno della struttura aziendale, per accertare il grado di probabilità di accadimento dell'evento e dell'impatto che il medesimo determinerebbe, individuando le metodologie di intervento che possono consentire di ridurlo;
- **aggiornamento della mappatura dei rischi** con il censimento delle aree e processi aziendali sensibili;
- **stesura della versione aggiornata del Modello 231.**

4.2.2 Esclusione di alcuni reati non applicabili alla realtà CSI

Il Risk Assessment condotto sul complesso delle attività aziendali, considerando anche i reati di più recente introduzione, ha portato ad escludere la possibilità di commissione dei seguenti reati:

- Reati nei confronti della P.A. - Concussione (art.317 c.p.) in quanto i dipendenti CSI non sono considerati pubblici ufficiali ai sensi di legge;
- Reati societari - Illecita influenza sull'assemblea (art.2636 c.c.) in quanto il capitale sociale di CSI è totalmente detenuto da Credit Suisse Group;
- Reati contro la personalità individuale (artt. 583-bis, 600, 600-bis, 600-ter, 600-quater, 600-quinquies, 601, 602 c.p.) perché reati difficilmente configurabili in ambito bancario;
- Reati di falso in materia di marchi e brevetti (art. 25-bis); Reati in materia di violazione della legge su diritto d'autore (art. 25-novies) ad esclusione dei reati previsti dall'art. 171 bis di cui alla n. 633 del 22 aprile 1941 che si ritengono invece astrattamente applicabili; Reati contro l'industria ed il commercio (art. 25-bis.1) in quanto loro commissione risulta difficilmente attuabile nell'ambito delle attività svolte da CSI.

Per completezza documentale, tali fattispecie di reato sono state riportate nella Parte Speciale del Modello, pur in mancanza di previsioni specifiche in relazione ai principi e regole di comportamento o ai conseguenti controlli da parte dell'Organismo di Vigilanza.

4.2.3 Inclusione di ulteriori fattispecie direate applicabili alla realtà di CSI nel corso dei Risk Assessment del 2011 e del 2015

Nel corso dell'attività di aggiornamento compiuta nel corso del 2011, sono state individuate ulteriori aree/processi aziendali sensibili alla commissione dei reati presupposto, per i quali si è proceduto alla mappatura e alla definizione o aggiornamento dell'insieme dei divieti e delle regole di comportamento generale e/o specifiche.

In particolare, l'individuazione del processo di gestione della formazione finanziata quale processo sensibile alla commissione dei reati inerenti i finanziamenti pubblici, ha reso necessario includere nel Modello le seguenti ulteriori fattispecie di reato:

- Malversazione a danno dello Stato (art.316-bis c.p.);
- Indebita percezione di erogazioni a danno dello Stato (art.316-ter c.p.);
- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.).

Tra i reati di più recente introduzione (confronta par. 4.2) sono stati individuate aree e processi a rischio per le fattispecie di reato elencate qui di seguito. Tali reati sono stati pertanto integrati nel Modello, definendo il relativo sistema di principi di comportamento, regole di condotta e divieti:

- Reati in materia di criminalità organizzata (artt. 416, 416-bis, 416-ter, 600, 601, 602, 630 c.p.; 407 c.p.p.; art. 12 d. lgs. 286/1998 e art. 74 d.P.R. 309/1990)
- Reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria (art. 377 bis c.p.).

Nel corso della successiva attività di aggiornamento compiuta nel 2015, sono state individuate ulteriori aree/processi aziendali sensibili alla commissione dei seguenti reati presupposto, per i quali si è proceduto alla mappatura e alla definizione o aggiornamento dell'insieme dei divieti e delle regole di comportamento generale e/o specifiche:

- corruzione tra privati (art. 2635 c.c.);
- autoriciclaggio (art. 648-ter.1 c.p.);
- impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 22, comma 12-bis, D.Lgs. 286/1998).

4.2.4 Approccio metodologico specifico in materia di salute e sicurezza sul luogo di lavoro

Con specifico riferimento ai rischi in materia di sicurezza e salute sul luogo di lavoro, l'*assessment* è stato effettuato tramite interviste con gli attori coinvolti nel processo di gestione del rischio, analisi documentale (organigramma per la sicurezza, atti di nomina dei delegati e responsabili del sistema di gestione della sicurezza, documento di valutazione dei rischi, procedure di emergenza, documentazione informativa e formativa, *gap analysis* predisposta a seguito della prima stesura del Modello ecc.) e l'effettuazione di un sopralluogo presso i luoghi di lavoro.

Pur confermando la validità dell'assunto che i rischi in materia di sicurezza sono, per loro natura, insiti in ogni ambito ed attività aziendale, si è ritenuto opportuno identificare e mappare le aree/processi a maggior rischio di commissione di tali reati, in quanto deputate specificatamente dalla legge e dall'organizzazione interna a presiedere al processo di gestione di tali rischi.

Si sottolinea, a questo proposito, come sia configurabile un vantaggio dell'ente nel cd *risparmio di spesa* ottenuto con il mancato impiego delle risorse economiche necessarie per l'organizzazione e gestione di un sistema di prevenzione e sicurezza, sia per quanto riguarda la dislocazione dei

soggetti garanti del sistema della sicurezza, che nell'adozione delle misure precauzionali, nonché in termini di risparmio di tempo e risorse.

4.2.5 Approccio metodologico specifico in materia di criminalità informatica

Con specifico riferimento alle analisi e valutazioni condotte in materia di criminalità informatica, per sua natura pervasiva di ogni ambito ed attività aziendale, l'attenzione è stata posta su quello che può essere definito quale il processo di "gestione della sicurezza informatica".

La valutazione è stata eseguita attraverso l'analisi documentale (in particolare, Information Security Policy, IT Risk Policy for Information Security, Titolarità, classificazione e trattamento delle informazioni, Uso corretto dell'IT) ed interviste con il Local Security Information Officer.

Dall'intervista emerge che, dalla stesura originale del Modello non vi sono state significative modifiche di tipo organizzativo ed è confermata l'adozione della metodologia COBIT (Control Objectives for Information and Related Technology) sviluppata da ISACA (Information Systems Audit and Control Association) per l'analisi degli aspetti di natura organizzativa ed in particolare degli standard ISO 38500 (Corporate governance for Information technology) e ISO 27001 (Information technology -- Security techniques -- Information security management systems -- Requirements) per la verifica della sussistenza delle condizioni che potrebbero favorire la commissione dei reati informatici di cui all'art. 24-bis del D.Lgs. 231/01.

Anche in questo caso, pur ritenendo che il rischio di commissione dei reati in materia di criminalità informatica sia insito in ogni ambito ed attività aziendale, in questa fase di aggiornamento si è ritenuto opportuno identificare e mappare le aree/processi a maggior rischio di commissione di tali reati, in quanto deputate specificatamente dalla legge e dall'organizzazione interne a presiedere alla gestione del processo di gestione di tali rischi.

4.3 Stesura del Modello 231

A conclusione dalla fase di *assessment*, sono stati redatti i seguenti documenti:

- Modello 231 nella presente versione di aggiornamento
- Tabella di mappatura dei reati e delle potenziali aree e processi aziendali sensibili
- Valutazione degli eventi a rischio individuati e rappresentazione grafica dei reati

5 IL MODELLO 231

5.1 Finalità e struttura del modello

Come anticipato in Premessa, il presente Modello 231 è parte integrante del "Regolamento di Direzione" di Credit Suisse Italy, ovvero un articolato sistema normativo aziendale che definisce per i dipendenti e i collaboratori, i promotori finanziari (Personal Banker), i doveri e gli obblighi da osservarsi nello svolgimento delle funzioni agli stessi assegnate.

Nello specifico, tuttavia, l'adozione del Modello 231, oltre a costituire un valido strumento di sensibilizzazione di tutti coloro che operano per conto di CSI, affinché tengano comportamenti corretti e lineari, è tesa in particolare alla creazione di un sistema di prescrizioni e strumenti organizzativi avente l'obiettivo di garantire che l'attività di CSI sia svolta nel pieno rispetto del Decreto 231 e di prevenire e sanzionare eventuali tentativi di porre in essere comportamenti a rischio di commissione di una delle fattispecie di reato previste dal Decreto stesso.

Pertanto il Modello 231 si propone come finalità quelle di:

- migliorare il sistema di Corporate Governance;
- predisporre un sistema strutturato ed organico di prevenzione e controllo finalizzato alla riduzione del rischio di commissione dei reati connessi all'attività aziendale;
- determinare, in tutti coloro che operano in nome e per conto di CSI nelle "aree di attività a rischio", la consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, in un illecito passibile di sanzioni sia a carico dell'autore della violazione (sul piano civilistico, disciplinare e, in taluni casi, penale) sia a carico della CSI (responsabilità amministrativa ai sensi del Decreto 231);
- informare tutti i soggetti rilevanti che operano a qualsiasi titolo in nome, per conto o comunque nell'interesse di CSI che la violazione delle prescrizioni contenute nel Modello 231 comporterà l'applicazione di apposite sanzioni oppure la risoluzione del rapporto contrattuale;
- ribadire che CSI non tollera comportamenti illeciti, di qualsiasi tipo ed indipendentemente da qualsiasi finalità, in quanto tali comportamenti (anche nel caso in cui CSI fosse apparentemente in condizione di trarne vantaggio) sono comunque contrari ai principi etici cui CSI intende attenersi;
- censurare fattivamente i comportamenti posti in essere in violazione del Modello 231 attraverso la comminazione di sanzioni disciplinari e/o contrattuali;
- consentire a CSI, grazie ad un'azione di monitoraggio sulle aree di attività a rischio, di intervenire tempestivamente, al fine di prevenire o contrastare la commissione dei reati stessi e sanzionare i comportamenti contrari al proprio Modello 231.

Il Modello 231 predisposto da CSI si fonda, pertanto, su un sistema strutturato ed organico di protocolli, nonché di attività di controllo che nella sostanza:

- individuano le aree/i processi di possibile rischio nell'attività aziendale vale a dire quelle attività nel cui ambito si ritiene più alta la possibilità che possano essere commessi i Reati;
- definiscono un sistema normativo interno, finalizzato alla prevenzione dei Reati, nei quali sono tra l'altro ricompresi:
 - un Codice di Condotta, che esprime gli impegni e le responsabilità etiche nella conduzione degli affari e delle attività aziendali;
 - un Codice Etico, che enuncia l'insieme dei principi, dei diritti, dei doveri e delle responsabilità della Banca rispetto a tutti i soggetti con i quali la stessa entra in relazione per il conseguimento del proprio oggetto sociale e che si propone di fissare standard di riferimento e norme comportamentali mirate a orientarne la condotta;
 - un sistema di deleghe, poteri e di procure per la firma di atti aziendali che assicuri una chiara e trasparente rappresentazione del processo di formazione e di attuazione delle decisioni;
 - procedure formalizzate, tese a disciplinare le modalità operative e di controllo nei Processi a Rischio;
- trovano il proprio presupposto in una struttura organizzativa coerente con le attività aziendali, volta ad ispirare e controllare la correttezza dei comportamenti, garantendo una chiara ed organica attribuzione dei compiti, applicando una giusta segregazione delle funzioni, assicurando che gli assetti voluti della struttura organizzativa siano realmente attuati, attraverso:
 - un organigramma formalmente definito, chiaro ed adeguato all'attività da svolgere;
 - una chiara definizione delle funzioni e delle responsabilità attribuite a ciascuna unità organizzativa;
 - un sistema di deleghe di funzioni interne e di procure a rappresentare CSI verso l'esterno che assicuri una chiara e coerente segregazione delle funzioni;
- individuano i processi di gestione e controllo delle risorse finanziarie nelle Aree a rischio;
- assicurano l'esistenza e la tracciabilità delle attività di controllo e supervisione compiute sulle transazioni aziendali;

- garantiscono la presenza di meccanismi di sicurezza in grado di assicurare un'adeguata protezione/accesso fisico-logico ai dati e ai beni aziendali;
- attribuiscono all'Organismo di Vigilanza il compito di vigilare sul funzionamento e sull'osservanza del Modello 231 e di proporre l'aggiornamento;
- definiscono i flussi informativi nei confronti dell'Organismo di Vigilanza;
- definiscono disposizioni idonee a sanzionare il mancato rispetto delle misure indicate nel Modello 231;
- definiscono le modalità di formazione del personale e la comunicazione interna in merito al contenuto del Decreto e del Modello 231 ed agli obblighi che ne conseguono.

Il Modello 231 è costituito da una Parte Generale e da una Parte Speciale.

Nella Parte Generale sono definiti gli elementi del Modello 231:

- il contesto normativo di riferimento;
- le logiche e la metodologia che hanno guidato la predisposizione del Modello 231;
- le finalità del Modello 231 e la sua relazioni con i sistemi normativi e di governance aziendale;
- gli specifici compiti e responsabilità dell' Organismo di Vigilanza;
- i flussi informativi verso l'Organismo di Vigilanza;
- il sistema sanzionatorio;
- le logiche formative;

Nella Parte Speciale sono indicate le Business Unit coinvolte, le singole aree di attività/processi a rischio individuati e gli specifici presidi ritenuti idonei a prevenire la commissione dei Reati previsti dal Decreto.

In fase di revisione del Modello, sia nel corso del 2011 che nel corso del 2015, si è ritenuto utile introdurre due elementi aggiuntivi all'organizzazione della Parte Speciale, che prevedono delle sezioni dedicate alla descrizione dei divieti e delle regole di comportamento inerenti specifici processi (*Procedure Specifiche*), nonché i possibili controlli dell'Organismo di Vigilanza (*Controlli dell'Organismo di Vigilanza*).

Tali sezioni sono state adottate per i processi più significativi allo scopo di rendere più agevole e focalizzata l'individuazione delle relative regole di comportamento e tipologie di controlli.

5.2 Destinatari del Modello 231

Le prescrizioni del Modello 231 sono indirizzate al legale rappresentante, ai soggetti apicali, ai dipendenti, e ai Collaboratori (ivi compresi i lavoratori somministrati e i lavoratori a progetto) e i promotori finanziari o "Personal Banker" di CSI, in quanto coinvolti nei Processi a Rischio, ai Consulenti, agli Appaltatori, nonché ai membri dell'Organismo di Vigilanza, in quanto non appartenenti alle categorie summenzionate.

I Destinatari del Modello 231 sono tenuti a rispettarne puntualmente tutte le disposizioni, anche in adempimento dei doveri di lealtà, correttezza e diligenza che scaturiscono dai rapporti giuridici instaurati con CSI.

E' fatto espresso divieto ai dipendenti ed agli organi sociali di CSI – in via diretta – nonché ai Collaboratori in forza di apposite clausole contrattuali di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reati contemplate dal Decreto 231;
- porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato contemplato nel Decreto 231, possano potenzialmente diventarlo;
- violare principi e disposizioni previsti nel presente documento.

CSI condanna qualsiasi comportamento difforme, oltre che dalla legge, dalle previsioni del Modello 231, anche qualora il comportamento sia realizzato nell'interesse di CSI ovvero con l'intenzione di arrecare ad essa un vantaggio.

5.3 Adozione, modifiche e integrazioni del Modello

Il Decreto prevede che sia l'organo dirigente ad adottare il Modello 231, rimettendo ad ogni ente il compito di individuare al proprio interno l'organo cui affidare tale compito.

In coerenza con quanto indicato dalla Linee Guida ABI, CSI ha individuato nel proprio Consiglio di Amministrazione l'Organo Dirigente deputato all'adozione del Modello. Il compito di vigilare sull'efficace attuazione del Modello è invece affidato, secondo quanto previsto dal Decreto, all'Organismo di Vigilanza (OdV).

Conseguentemente, essendo il presente documento un atto di emanazione dell'Organo Dirigente (in conformità alle prescrizioni dell'art. 6 co. 1 lett. a) del Decreto) le successive modifiche ed integrazioni di carattere sostanziale dello stesso sono rimesse coerentemente alla competenza dello stesso Consiglio di Amministrazione.

Fra le modifiche di carattere sostanziale rientrano, a titolo esemplificativo e non esaustivo:

- integrazione della parte speciale del presente documento con ulteriori sezioni dedicate a nuove eventuali categorie di reato applicabili alla realtà CSI;
- soppressione di alcune parti del presente documento;
- modifica dei compiti dell'OdV;
- individuazione di un OdV diverso da quello attualmente previsto;
- aggiornamento/modifica/integrazione dei principi di controllo e delle regole comportamentali.

E' peraltro riconosciuta all'Amministratore Delegato la facoltà di apportare eventuali modifiche o integrazioni al presente documento di carattere esclusivamente formale, a condizione che il contenuto rimanga invariato nella sostanza, nonché apportare eventuali integrazioni, modifiche ed aggiornamenti agli Allegati.

Di tali modifiche o integrazioni dovrà essere prontamente informato il Consiglio di Amministrazione e l'OdV.

5.4 Formazione

La formazione del personale ai fini dell'attuazione del Modello 231 è di competenza del CdA che ha individuato nell'Unità Organizzativa Human Resource - Training & Development la funzione a cui affidarne l'organizzazione.

Tali risorse procedono in coordinamento con l'OdV, che ne valuta l'efficacia in termini di pianificazione, contenuti, aggiornamento, tempistiche, modalità e identificazione dei partecipanti, organizzazione delle sessioni di formazione.

La partecipazione alle suddette attività formative da parte dei soggetti individuati è obbligatoria: conseguentemente, la mancata partecipazione sarà sanzionata ai sensi del Sistema Disciplinare contenuto nel Modello 231.

La formazione deve fornire informazioni almeno in riferimento: al quadro normativo di riferimento (D. Lgs. 231/2001 e Linee Guida di Categoria, etc.); al Modello 231 adottato da CSI; al Codice di Condotta; a casi aziendali di applicazione della normativa; ai presidi e protocolli introdotti a seguito dell'adozione del Modello 231 stesso.

E' prevista una formazione on-line rivolta a tutti i dipendenti e Personal Banker in organico presso CSI al momento dell'adozione del Modello 231.

Della formazione effettuata dovrà essere tenuta puntuale registrazione.

Infine, la pianificazione della formazione deve prevedere delle sessioni periodiche, sempre attraverso la modalità on-line, che garantiscano un costante programma di aggiornamento.

6 ORGANISMO DI VIGILANZA

6.1 Identificazione dell'OdV

In base al Decreto 231, l'organismo che deve vigilare sul funzionamento e sull'osservanza del Modello 231 deve essere dotato di autonomi poteri di vigilanza e controllo.

Sulla base di questo presupposto e delle indicazioni contenute nelle linee guida ABI e Confindustria, il CdA di CSI ha ritenuto opportuno costituire un organo collegiale per svolgere il ruolo di OdV.

L'Organismo di Vigilanza è composto da non meno di 3 componenti di cui almeno 1 sia soggetto esterno al gruppo.

L'OdV avrà comunque la facoltà di utilizzare le funzioni, interne (come l'Audit Department di Gruppo) o esterne, per lo svolgimento delle attività di controllo/verifica o di contenuto più specificamente tecnico.

A ulteriore garanzia di autonomia e in coerenza con quanto previsto dalle Linee Guida dell'ABI, nonché dalle Linee Guida Confindustria, in sede di nomina dei componenti dell'OdV il CdA dovrà dotare lo stesso di un proprio budget di spesa.

I componenti dell'OdV sono nominati dal CdA.

La composizione dell'OdV dovrà comunque essere tale da garantire la sua piena autonomia ed indipendenza nell'espletamento delle proprie funzioni, in ossequio ai dettami del Decreto 231, nonché la continuità d'azione dello stesso.

6.2 Modalità di nomina e revoca

L'OdV è nominato dal CdA. Nello stesso modo il CdA provvede anche alla nomina del Presidente dell'OdV.

Il perfezionamento della nomina dei membri dell'OdV si determina con la dichiarazione di accettazione da parte di questi, resa a verbale del CdA, oppure con la sottoscrizione per accettazione, da parte degli stessi, della copia dell'estratto di detta determinazione.

Il CdA valuta periodicamente l'adeguatezza dell'OdV in termini di struttura organizzativa e di poteri conferiti e può, in qualunque momento, revocare il mandato ad uno (o a tutti) i membri dell'OdV, sempre che sussista una giusta causa, come meglio specificato al paragrafo successivo.

Il CdA provvede, prima di ogni nuova nomina, a verificare la sussistenza dei requisiti espressamente richiesti dal Decreto 231 per ciascun membro dell'OdV, nonché degli altri requisiti citati nel presente capitolo.

E' responsabilità del CdA provvedere alla tempestiva nomina del membro dell'OdV decaduto o revocato o, comunque, cessato.

I membri dell'OdV potranno dimettersi dalla carica e, d'altra parte, essere rieletti alla scadenza del loro mandato.

6.3 Cause di ineleggibilità e motivi di revoca

La nomina quale componente dell'OdV, è condizionata alla presenza dei requisiti soggettivi dell'onorabilità, integrità, rispettabilità e professionalità, nonché all'assenza di cause di incompatibilità con la nomina stessa quali quelli descritti di seguito.

In particolare, all'atto del conferimento dell'incarico, il soggetto designato a ricoprire la carica di membro dell'OdV deve rilasciare una dichiarazione nella quale attesta l'assenza dei seguenti motivi di incompatibilità:

- conflitti di interesse, anche potenziali, con la CSI tali da pregiudicare l'indipendenza richiesta dal ruolo e dai compiti propri dell'OdV;
- funzioni di amministratore – nei tre esercizi precedenti alla nomina quale membro dell'OdV ovvero all'instaurazione del rapporto di consulenza/collaborazione con lo stesso Organismo – di imprese sottoposte a fallimento, liquidazione coatta amministrativa o altre procedure concorsuali;
- rapporto di pubblico impiego presso amministrazioni centrali o locali nei tre anni precedenti alla nomina quale membro dell'OdV ovvero all'instaurazione del rapporto di consulenza/collaborazione con lo stesso Organismo;
- sentenza di condanna anche non passata in giudicato, ovvero sentenza di applicazione della pena su richiesta (il c.d. patteggiamento), in Italia o all'estero, per i delitti richiamati dal Decreto 231 o delitti ad essi assimilabili, ovvero per altri delitti;
- condanna, con sentenza anche non passata in giudicato, a una pena che importa l'interdizione, anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese.

Le regole sopra descritte si applicano anche in caso di nomina di un componente dell'OdV in sostituzione di altro membro dell'organismo stesso.

La revoca di uno o di tutti i membri dell'OdV e l'attribuzione di tali poteri ad altri soggetti, potrà avvenire soltanto per giusta causa, anche legata ad interventi di ristrutturazione organizzativa della CSI, mediante un'apposita determinazione del CdA e con l'approvazione del Collegio Sindacale.

A tale proposito, per "giusta causa" di revoca dei poteri connessi con l'incarico di membro dell'OdV potrà intendersi, a titolo meramente esemplificativo:

- la perdita dei requisiti soggettivi di onorabilità, integrità, rispettabilità, professionalità e indipendenza presenti in sede di nomina;
- il sopraggiungere di un motivo di incompatibilità;
- una grave negligenza nell'assolvimento dei compiti connessi con l'incarico quale (a titolo meramente esemplificativo): l'omessa redazione della relazione informativa periodica o del verbale riepilogativo annuale sull'attività svolta al CdA e l'omessa redazione del piano delle attività;
- l'"omessa o insufficiente vigilanza" da parte dell'OdV, secondo quanto previsto dall'art. 6, comma 1, lett. d), del Decreto 231;

- l'attribuzione di funzioni e responsabilità operative all'interno dell'organizzazione aziendale incompatibili con i requisiti di "autonomia e indipendenza" e "continuità di azione" propri dell'OdV.

In casi di particolare gravità, il CdA potrà comunque disporre, sentito il parere del Collegio Sindacale, la sospensione dei poteri dell'OdV e la nomina di un Organismo ad interim.

6.4 Durata in carica dell'OdV

L'OdV dura in carica 3 esercizi, durante i quali i suoi membri potranno dimettersi dalla carica.

L'OdV decade alla data dell'assemblea convocata per l'approvazione del bilancio relativo all'ultimo esercizio della sua carica, pur continuando a svolgere ad interim le proprie funzioni fino a nuova nomina dei componenti dell'organismo stesso.

Alla scadenza del loro mandato i membri potranno, essere rieletti.

6.5 Funzioni dell'OdV

L'OdV è completamente autonomo nell'esplicazione dei suoi compiti e le sue determinazioni sono insindacabili. In particolare l'OdV deve:

- vigilare sull'osservanza del Modello 231 da parte dei soggetti destinatari;
- vigilare sull'efficienza e adeguatezza del Modello 231 in relazione alla struttura aziendale ed alla effettiva capacità di prevenire la commissione dei reati;
- proporre e sollecitare l'aggiornamento del Modello 231, laddove si riscontrino esigenze di adeguamento dello stesso in relazione a mutate condizioni aziendali, normative, o di contesto esterno.

L'OdV deve inoltre operare:

- ex-ante (adoperandosi ad esempio l'informazione del personale);
- continuativamente (attraverso l'attività di monitoraggio, di vigilanza, di revisione e di aggiornamento);
- ex-post (analizzando cause, circostanze che abbiano portato alla violazione delle prescrizioni del Modello 231 o alla commissione del reato).

Per un efficace svolgimento delle predette funzioni, all'OdV sono affidati i seguenti compiti e poteri:

- verificare periodicamente la mappa dei Processi a Rischio al fine di garantire l'adeguamento ai mutamenti dell'attività e/o della struttura aziendale;
- verificare periodicamente il flusso informativo nei propri confronti: raccogliere, elaborare e conservare le informazioni rilevanti in ordine al Modello;
- verificare periodicamente l'effettiva applicazione delle procedure aziendali di controllo nelle aree di attività a rischio e sulla loro efficacia;
- verificare periodicamente – con il supporto delle altre funzioni competenti – il sistema di deleghe in vigore, raccomandando modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti al responsabile di funzione od ai sub responsabili;
- verificare l'adozione degli interventi a soluzione delle criticità in termini di sistemi di controllo interno rilevate in sede di risk assessment;

- verificare periodicamente, con il supporto delle altre funzioni competenti, la validità di opportune clausole finalizzate:
 - all'osservanza da parte dei Destinatari dei contenuti del Modello 231 e del Codice di Condotta;
 - alla possibilità per la Banca di effettuare efficaci azioni di controllo nei confronti dei Destinatari del Modello al fine di verificare il rispetto delle prescrizioni in esso contenute;
 - all'attuazione di meccanismi sanzionatori (quali la risoluzione del contratto nei riguardi di Consulenti esterni, di Personal Banker etc.) qualora si accertino violazioni delle prescrizioni.
- effettuare periodicamente verifiche su operazioni o atti specifici posti in essere nell'ambito dei Processi a Rischio;
- verificare l'efficacia dei sistemi di raccordo tra i soggetti coinvolti nel sistema di controllo ai sensi del D.Lgs. 231/01 e delle normative speciali in materia di antiriciclaggio;
- esaminare le segnalazioni concernenti eventuali violazioni del Modello riguardanti la salute e sicurezza sul lavoro;
- verificare l'efficacia del sistema di flussi informativi rivolti all'OdV stesso, al Datore di Lavoro e RSPP;
- verificare l'efficacia dei sistemi di raccordo tra i soggetti coinvolti nel sistema di controllo ai sensi del D.Lgs. 231/01 e delle normative speciali in materia di sicurezza e salute sul luogo di lavoro;
- effettuare efficaci azioni di controllo nei confronti dei Destinatari del Modello al fine di verificare il rispetto delle prescrizioni in esso contenute, con particolare riferimento ai soggetti terzi (quali Appaltatori, etc.);
- verificare periodicamente – con il supporto delle altre funzioni competenti – l'osservanza delle norme aziendali in materia di gestione della sicurezza informatica;
- condurre indagini interne e svolgere attività ispettiva per accertare presunte violazioni delle prescrizioni del Modello 231;
- monitorare l'adeguatezza del sistema disciplinare previsto per i casi di violazione delle regole definite dal Modello 231;
- coordinarsi con le altre funzioni aziendali, nonché con gli altri organi di controllo, anche attraverso apposite riunioni, per il migliore monitoraggio delle attività in relazione ai protocolli stabiliti dal Modello 231, o per l'individuazione di nuovi Processi/Aree a Rischio, nonché, in generale, per la valutazione dei diversi aspetti attinenti all'attuazione del Modello 231;
- coordinarsi e cooperare con i soggetti responsabili della tutela della sicurezza e salute dei lavoratori al fine di garantire che il sistema di controllo ai sensi del Decreto 231 sia integrato con il sistema di controllo predisposto in conformità alle normative speciali per la sicurezza sui luoghi di lavoro;
- coordinarsi con i responsabili delle funzioni aziendali al fine di promuovere iniziative per la diffusione della conoscenza (anche in riferimento nello specifico all'organizzazione di corsi di formazione) e della comprensione dei principi del Modello 231 e per assicurare la predisposizione della documentazione organizzativa interna necessaria al funzionamento dello stesso, contenente istruzioni, chiarimenti o aggiornamenti;
- effettuare verifiche periodiche sul contenuto e sulla qualità dei programmi di formazione.

A tal fine l'OdV avrà facoltà di:

- emanare disposizioni ed ordini di servizio intesi a regolare l'attività dell'OdV stesso;
- accedere ad ogni e qualsiasi documento aziendale rilevante per lo svolgimento delle funzioni attribuite all'OdV ai sensi del Decreto 231;

- impartire direttive generali e specifiche alle diverse strutture aziendali, anche di vertice, al fine di ottenere da queste ultime le informazioni ritenute necessarie per l'assolvimento dei propri compiti, in modo che sia assicurata la tempestiva rilevazione di eventuali violazioni del Modello 231;
- effettuare verifiche periodiche sulla base di un proprio piano di attività o anche interventi spot non programmati in detto piano, ma, comunque, ritenuti necessari all'espletamento dei propri compiti.

L'OdV ha il compito inoltre di proporre all'Organo Dirigente eventuali modifiche e/o integrazioni delle suddette aree di attività/Processi a Rischio affinché questo provveda ad adeguare conseguentemente il Modello ed ad aggiornare in particolare la presente Parte Speciale.

Nello svolgimento dei compiti che gli competono, l'OdV avrà comunque la facoltà di ricorrere al supporto di collaboratori esterni, identificabili in soggetti appartenenti a qualsiasi funzione aziendale di CSI che di volta in volta si rendesse utile coinvolgere per il perseguimento dei fini specificati e/o di consulenti terzi.

I collaboratori dell'OdV, su indicazione dell'OdV stesso, possono, anche individualmente, procedere alle attività di vigilanza ritenute opportune per il funzionamento e l'osservanza del Modello 231.

I soggetti appartenenti ad una funzione aziendale, nell'espletamento dell'incarico ad essi conferito in qualità di collaboratori dell'OdV, sono esonerati dallo svolgimento delle loro funzioni operative aziendali e rispondono, gerarchicamente e funzionalmente, esclusivamente all'OdV.

L'OdV provvederà a dotarsi di un proprio Regolamento che ne assicuri l'organizzazione e gli aspetti di funzionamento quali, ad esempio, la periodicità degli interventi ispettivi, le modalità di deliberazione, le modalità di convocazione e verbalizzazione delle proprie adunanze, la risoluzione dei conflitti d'interesse e le modalità di modifica/revisione del Regolamento stesso.

Inoltre, nell'ambito del proprio Regolamento, l'OdV potrà espressamente prevedere dei momenti formalizzati di incontro e confronto, in particolare con:

- gli attori rilevanti in materia di sistema di controllo interno;
- gli attori rilevanti nell'ambito degli adempimenti in materia di antiriciclaggio;
- gli attori rilevanti in materia di sistema di gestione della salute e sicurezza sul luogo di lavoro.

Obiettivo di detti incontri sarà principalmente il confronto ed il coordinamento con i soggetti coinvolti in c.d. prima linea nell'implementazione del sistema di controllo, ciascuno secondo l'area di propria pertinenza, al fine di consentire all'OdV di cogliere opportunità di miglioramento dei presidi in essere ai fini dell'efficacia del Modello 231. In tale ottica sarà cura dell'OdV verificare con gli stessi l'efficacia dei flussi informativi nei suoi confronti, così come definiti al paragrafo 4.6 "Obblighi di informazione verso l'Organismo di Vigilanza".

L'OdV provvederà a disciplinare le modalità operative e la periodicità di organizzazione di detti incontri, individuando i soggetti di volta in volta coinvolti, nonché l'ordine del giorno degli stessi.

L'OdV, inoltre, provvederà a dotarsi di un Piano delle Attività che intende svolgere per adempiere ai compiti assegnatigli, da comunicare al CdA.

6.6 Obblighi di informazione verso l'Organismo di Vigilanza

Al fine di agevolare l'attività di vigilanza sull'effettività e sull'efficacia del Modello 231, l'OdV è destinatario di:

- *segnalazioni* relative a violazioni, presunte o effettive, del Modello 231 (di seguito **Segnalazioni**);
- *informazioni* utili e necessarie allo svolgimento dei compiti di vigilanza affidati all'OdV stesso (di seguito **Informazioni**).

Deve essere permesso all'OdV di accedere ad ogni tipo di informazione utile al fine dello svolgimento della sua attività. Ne deriva di converso l'obbligo per l'OdV di mantenere segrete tutte le informazioni acquisite.

Nello specifico, **tutti i Destinatari** dovranno tempestivamente segnalare all'OdV casi di violazione, anche presunta, del Modello 231.

Tali Segnalazioni dovranno essere sufficientemente precise e circostanziate e riconducibili ad un definito evento o area; si precisa che tali Segnalazioni potranno riguardare qualsiasi ambito aziendale rilevante ai fini dell'applicazione del D.Lgs. 231/2001 e del Modello 231 vigente, ivi incluse le violazioni del Modello 231 rilevanti ai fini della sicurezza e salute sul lavoro.

Si precisa altresì che è facoltà anche dei Rappresentanti dei Lavoratori per la sicurezza, laddove tale funzione non sia svolta da un soggetto rientrante tra i Destinatari del Modello 231, di inviare tali Segnalazioni all'OdV.

Al ricevimento di una Segnalazione riguardante una violazione, anche presunta, del Modello 231 rilevante ai fini della sicurezza e salute sul lavoro, sarà onere dell'OdV verificare che il mittente abbia precedentemente o contestualmente informato anche il Datore di Lavoro e il Responsabile del Servizio di Prevenzione e Protezione.

In ogni caso al fine di agevolare le attività di vigilanza che gli competono, l'OdV deve ottenere tempestivamente le seguenti Informazioni ritenute utili a tale scopo:

<u>Informazioni</u>	<u>Chi fornisce le informazioni</u>
<ul style="list-style-type: none"> le criticità, anomalie o atipicità riscontrate dalle funzioni aziendali nell'attuazione del Modello 231; 	Responsabili di tutti gli uffici, tramite segnalazione alla casella email dell'OdV (# 231 italy)
<ul style="list-style-type: none"> i provvedimenti e/o notizie formalmente provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini nei confronti di Credit Suisse Italy (S.p.A.) e/o di altre Società appartenenti al Credit Suisse Group per i Reati di cui al Decreto 231; 	Legal, Compliance, Financial Accounting
<ul style="list-style-type: none"> le comunicazioni interne ed esterne riguardanti qualsiasi fattispecie che possa essere messa in collegamento con ipotesi di reato di cui al Decreto 231; 	Legal, Compliance, Internal Audit, Operation Risk Management
<ul style="list-style-type: none"> le richieste di assistenza legale inoltrate dai dipendenti in caso di avvio di procedimento giudiziario per i Reati; 	Human Resource
<ul style="list-style-type: none"> le commissioni di inchiesta o le relazioni interne dalle quali emergano responsabilità per le ipotesi di reato di cui al Decreto 231; 	Internal Audit, Compliance

<ul style="list-style-type: none"> le notizie relative ai procedimenti disciplinari svolti con riferimento a violazioni del Modello 231 e alle eventuali sanzioni irrogate (ivi compresi i provvedimenti verso i dipendenti) ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni; 	Human Resource
<ul style="list-style-type: none"> le notizie relative a cambiamenti dell'assetto organizzativo; 	Human Resource, BPPM
<ul style="list-style-type: none"> gli aggiornamenti del sistema delle deleghe e delle procure (ivi incluso il sistema poteri e deleghe in materia di sicurezza e salute sul lavoro); 	Legal, BPPM
<ul style="list-style-type: none"> le notizie relative a cambiamenti organizzativi dei ruoli chiave in materia di sicurezza e salute sul luogo di lavoro (es: cambiamenti in merito a ruoli, compiti e soggetti delegati alla tutela dei lavoratori); 	il Datore di lavoro, il Delegato del Datore di lavoro, i Dirigenti, il Responsabile del Servizio di Prevenzione e Protezione e il Medico competente
<ul style="list-style-type: none"> modifiche al sistema normativo in materia di sicurezza e salute sul luogo di lavoro; 	il Datore di lavoro, il Delegato del Datore di lavoro, i Dirigenti, il Responsabile del Servizio di Prevenzione e Protezione e il Medico competente
<ul style="list-style-type: none"> la copia di bilancio relativo a CSI; 	Financial Accounting
<ul style="list-style-type: none"> copia dei verbali dei Comitati previsti dal Regolamento di Direzione. 	Il Presidente di ogni comitato, per il tramite del Segretario
<ul style="list-style-type: none"> informazioni sulle aree rilevanti in tema di reati in materia di criminalità informatica 	Responsabile IT
<ul style="list-style-type: none"> Qualunque operazione (attiva o passiva) in deroga o con valori fuori standard. A titolo esemplificativo e non esaustivo: <ul style="list-style-type: none"> acquisti diretti tempi di pagamento a fornitori fuori policy assunzioni di dipendenti su segnalazione interna o esterna erogazione credito a valori economici fuori policy⁴ 	Tutte le funzioni.

E' inoltre a disposizione di tutti i dipendenti e dei collaboratori una *hotline* attiva 24 ore su 24, sette giorni alla settimana, che consente di effettuare una segnalazione iniziale di potenziali comportamenti scorretti. Le modalità per contattare l'*Integrity Hotline* sono riportate nel Codice di Condotta. Le segnalazioni inoltrate tramite l'*Integrity Hotline* sono trasmesse, qualora pertinenti, all'Organismo di Vigilanza.

Al fine di agevolare l'accesso da parte dell'OdV al maggior numero possibile di informazioni, CSI garantisce la tutela di qualunque segnalante contro ogni forma di ritorsione, discriminazione o penalizzazione, fatti salvi gli obblighi di legge e la tutela dei diritti di CSI o delle persone accusate erroneamente e/o in mala fede.

⁴ Cadenza e soglie di rischio saranno decisi dall'ODV nell'ambito delle sue competenze.

L'OdV valuterà le Segnalazioni ricevute con discrezionalità e responsabilità, provvedendo ad indagare anche ascoltando l'autore della Segnalazione e/o il responsabile della presunta violazione, motivando per iscritto la ragione dell'eventuale autonoma decisione di non procedere e dandone comunque comunicazione al CdA nell'ambito del processo di reporting (si rimanda sul tema al successivo Paragrafo 6.7).

Sarà infine cura dell'OdV, definire e diffondere nei confronti dei Destinatari eventuali istruzioni, regole e meccanismi operativi specifici finalizzati a raccogliere ulteriori informazioni rilevanti relative alle attività svolte nelle Aree/Processi a rischio e ritenute particolarmente sensibili (quali, a puro titolo esemplificativo: l'assegnazione di incarichi a Consulenti; l'assegnazione di incarichi ad Appaltatori; l'avvio di contenziosi contrattuali; l'avvio di contenziosi con dipendenti o comunque attinenti l'area dei rapporti di lavoro; l'assunzione di nuovi risorse in capo a CSI; etc.). In particolare tali informazioni ed elementi rilevanti potranno essere contenuti nella reportistica già attualmente prodotta a livello aziendale e/o di Gruppo, o, eventualmente, potranno essere raccolti attraverso altri strumenti/format/canali/modalità definiti dall'OdV stesso.

6.7 Reporting dell'OdV

L'OdV riferisce in merito all'attuazione del Modello 231 e alle eventuali criticità, direttamente al CdA.

L'OdV, nei confronti del CdA, ha la responsabilità di:

- comunicare, all'inizio di ciascun esercizio, il Piano delle Attività, che intende svolgere per adempiere ai compiti assegnatigli;
- comunicare periodicamente, ed almeno semestralmente, lo stato di avanzamento del Piano delle attività, ed eventuali cambiamenti apportati allo stesso, motivandoli;
- segnalare tempestivamente qualsiasi violazione del Modello 231 oppure condotte illegittime e/o illecite, di cui sia venuto a conoscenza per Segnalazione da parte dei Destinatari che l'OdV ritenga fondate o che abbia accertato;
- redigere, almeno una volta l'anno, una relazione riepilogativa delle attività svolte nei precedenti dodici mesi e dei risultati delle stesse, degli elementi di criticità e delle violazioni del Modello 231, nonché delle proposte relative ai necessari aggiornamenti del Modello 231 da porre in essere.

Il CdA ha la facoltà di convocare in qualsiasi momento l'OdV, il quale, a sua volta, ha la facoltà di richiedere, attraverso le funzioni o i soggetti competenti, la convocazione del predetto organo per motivi urgenti e di particolare gravità.

L'OdV potrà, inoltre, comunicare i risultati dei propri accertamenti ai responsabili delle funzioni qualora dalle verifiche svolte scaturiscano carenze, comportamenti o azioni non in linea con il Modello 231. In tal caso, sarà necessario che l'OdV ottenga dai responsabili dei processi medesimi un piano delle azioni da intraprendere, con relativa tempistica, al fine di impedire il ripetersi di tali circostanze.

Al ricevimento di una Segnalazione relativa alla tutela della salute e sicurezza sul lavoro, l'OdV provvederà ad informare il Datore di Lavoro e il Responsabile del Servizio di Prevenzione e Protezione, qualora il mittente della Segnalazione non vi abbia già provveduto. L'OdV provvederà altresì ad informare tempestivamente il CdA in merito alle Segnalazioni ritenute fondate e/o accertate.

Al ricevimento di una Segnalazione rilevanti ai fini Antiriciclaggio, l'OdV provvederà ad informare il Responsabile Antiriciclaggio CSI e il Responsabile Compliance CS, qualora il mittente della Segnalazione non vi abbia già provveduto. L'OdV provvederà altresì ad informare tempestivamente il CdA in merito alle Segnalazioni ritenute fondate e/o accertate.

Al ricevimento di una Segnalazione rilevanti ai fini di Market Abuse, l'OdV provvederà ad informare il Responsabile Compliance CS, qualora il mittente della Segnalazione non vi abbia già provveduto. L'OdV provvederà altresì ad informare tempestivamente il CdA in merito alle Segnalazioni ritenute fondate e/o accertate.

6.8 Conservazione delle informazioni

Tutte le Informazioni, Segnalazioni, rapporti e altri documenti raccolti e/o predisposti in applicazione del presente Modello 231 sono conservati dall'OdV, a cura del Segretario, in un apposito archivio (informatico e/o cartaceo), per un periodo di 10 anni.

La gestione e custodia dell'archivio è in carico all'OdV fermo restando l'osservanza delle disposizioni in materia di riservatezza dei dati personali e dei diritti da essa garantiti in favore degli interessati, non accessibile da altri. L'accesso all'archivio è consentito esclusivamente ai membri dell'OdV e al CdA.

7 SISTEMA DISCIPLINARE

Il Decreto 231 prevede che sia predisposto un *“sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello”* sia per i soggetti in posizione apicale, che per i soggetti sottoposti ad altrui direzione.

L'esistenza di un sistema di sanzioni applicabili in caso di mancato rispetto dei protocolli previsti dal Modello 231 è, infatti, indispensabile per garantire l'effettività del Modello 231 stesso.

L'applicazione delle sanzioni in questione deve restare del tutto indipendente dallo svolgimento e dall'esito di eventuali procedimenti penali avviati dall'autorità giudiziaria, nel caso in cui il comportamento da censurare valga anche ad integrare una fattispecie di reato rilevante ai sensi del Decreto 231. Infatti, le regole di condotta imposte dal Modello 231 sono assunte dall'azienda in piena autonomia indipendentemente dal fatto che eventuali condotte possano costituire reato e che l'autorità giudiziaria intenda perseguire tale illecito.

Il sistema disciplinare definito potrà essere applicato anche ai componenti dell'OdV, relativamente alle funzioni ad essi attribuite dal presente Modello.

7.1 Violazioni del Modello

Costituiscono violazioni del Modello:

1. comportamenti che integrino, direttamente o indirettamente, le fattispecie di reato contemplate nel Decreto 231;
2. comportamenti che, sebbene non configurino uno dei Reati, siano diretti in modo univoco alla loro commissione;
3. comportamenti non conformi alle procedure richiamate nel Modello 231 al fine di ridurre il rischio di commissione di uno degli illeciti considerati dal Decreto 231.
4. comportamenti non conformi ai protocolli previsti nel Modello 231 o richiamati dal Modello 231 e, in particolare:

- in relazione al rischio di commissione di un reato nei confronti della Pubblica Amministrazione, i comportamenti in violazione dei principi di controllo e di comportamento elencati nella Parte Speciale 8;
 - in relazione al rischio di commissione di un reato societario, ivi compreso il reato di corruzione tra privati, i comportamenti in violazione dei principi di controllo e di comportamento elencati nella Parte Speciale 9;
 - in relazione al rischio di commissione di un reato di falsità in monete, carte di pubblico credito e valori di bollo, i comportamenti in violazione dei principi di controllo e di comportamento elencati nella Parte Speciale 10;
 - in relazione al rischio di commissione di un reato in tema di manipolazione del mercato e di abuso di informazioni privilegiate i comportamenti in violazione dei principi di controllo e di comportamento elencati nella Parte Speciale 11;
 - in relazione al rischio di commissione di un reato transnazionale, i comportamenti in violazione dei principi di controllo e di comportamento elencati alla Parte Speciale 12;
 - in relazione al rischio di commissione di un reato con finalità di terrorismo, i comportamenti in violazione dei principi di controllo e di comportamento elencati nella Parte Speciale 13; in relazione al rischio di violazione delle norme stabilite in materia di tutela della salute e sicurezza sul lavoro da cui possa derivare l'evento di infortunio o della malattia professionale comportanti il reato di omicidio colposo o di lesioni colpose gravi o gravissime, i comportamenti in violazione dei principi di controllo e di comportamento elencati nella Parte Speciale 15;
 - in relazione ai reati di criminalità informatica i comportamenti in violazione dei principi di controllo e di comportamento elencati nella Parte Speciale 16;
 - in relazione ai reati in tema di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio, i comportamenti in violazione dei principi di controllo e di comportamento elencati nella Parte Speciale 17;
 - in relazione ai reati di criminalità organizzata i comportamenti in violazione dei principi di controllo e di comportamento elencati nella Parte Speciale 18;
 - in relazione ai delitti in violazione al reato di induzione a non rendere dichiarazioni o rendere dichiarazioni mendaci, i comportamenti in violazione dei principi di controllo e di comportamento elencati nella Parte Speciale 21;
 - in relazione al reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare, i comportamenti in violazione dei principi di controllo e di comportamento elencati nella Parte Speciale 22;
5. comportamento non collaborativo nei confronti dell'OdV, consistente a titolo esemplificativo e non esaustivo, nel rifiuto di fornire le informazioni o la documentazione richiesta, nel mancato rispetto delle direttive generali e specifiche rivolte dall'OdV al fine di ottenere le informazioni ritenute necessarie per l'assolvimento dei propri compiti, nella mancata partecipazione senza giustificato motivo alle visite ispettive programmate dall'OdV, nella mancata partecipazione agli incontri di formazione;
6. violazione degli obblighi di informazione verso l'OdV indicati nel paragrafo 6.6 della Parte Generale.

Questa elencazione delle violazioni ha carattere esemplificativo e non si deve, dunque, ritenere completa, essendo possibili violazioni di tipo diverso rispetto a quelle contenute nell'elenco.

Qualsiasi tipo di violazione delle regole comportamentali contenute nel Modello 231 autorizza l'OdV a richiedere al soggetto titolare del potere disciplinare di CSI, l'irrogazione di una delle sanzioni elencate nei successivi paragrafi del presente Capitolo del Modello 231, determinata sulla base della gravità della violazione commessa e del comportamento tenuto prima (e.g. eventuali precedenti violazioni commesse) e dopo il fatto (e.g. comunicazione all'OdV dell'avvenuta irregolarità) dall'autore della violazione.

La gravità delle violazioni del Modello 231 sarà valutata sulla base delle seguenti circostanze:

- la presenza e l'intensità dell'elemento intenzionale;
- la presenza e intensità della condotta negligente, imprudente, imperita;
- la presenza e intensità della condotta recidiva;
- l'entità del pericolo e/o delle conseguenze della violazione per CSI;
- l'entità del pericolo e/o delle conseguenze della violazione per le persone destinatarie della normativa in materia di tutela della salute e della sicurezza sui luoghi di lavoro, nonché per CSI;
- la prevedibilità delle conseguenze della condotta in violazione;
- i tempi e i modi della violazione;
- le circostanze nelle quali la violazione ha avuto luogo.

7.2 Misure nei confronti dei dipendenti

La violazione delle singole regole comportamentali di cui al presente Modello 231 da parte dei dipendenti soggetti al CCNL per i quadri direttivi e le aree professionali dipendenti delle aziende di credito, finanziarie e strumentali (19 gennaio 2012) costituisce illecito disciplinare.

I provvedimenti disciplinari irrogabili nei riguardi di detti lavoratori - nel rispetto delle procedure previste dall'articolo 7 della legge 30 maggio 1970, n. 300 (Statuto dei Lavoratori) ed eventuali normative speciali applicabili - sono quelli previsti dall'apparato sanzionatorio di cui agli artt. 34 e ss. del suddetto CCNL, e precisamente (art. 40):

- a. rimprovero verbale;
- b. rimprovero scritto;
- c. la sospensione dal servizio e dal trattamento economico per un periodo non superiore a 10 giorni;
- d. il licenziamento per notevole inadempimento degli obblighi contrattuali del prestatore di lavoro (giustificato motivo);
- e. il licenziamento per una mancanza così grave da non consentire la prosecuzione anche provvisoria del rapporto (giusta causa).

Quando sia richiesto dalla natura della mancanza o dalla necessità di accertamenti in conseguenza della medesima, la CSI - in attesa di deliberare il definitivo provvedimento disciplinare - può disporre l'allontanamento temporaneo del lavoratore/lavoratrice dal servizio per il tempo strettamente necessario.

In ogni caso, delle sanzioni irrogate e/o delle violazioni accertate, la funzione aziendale competente terrà sempre informato l'OdV.

In particolare, con riferimento alle violazioni del Modello 231 poste in essere dai dipendenti di CSI, si prevede che:

1. incorre nei provvedimenti di **rimprovero verbale o scritto** secondo la gravità della violazione, il dipendente che violi i protocolli interni previsti dal presente Modello 231 o adottati, nell'espletamento di attività nei Processi/Aree a rischio, un comportamento in violazione delle prescrizioni del Modello 231 stesso, purché tale condotta non determini l'applicazione di misure previste dal Decreto 231;
2. incorre nel provvedimento di **sospensione dal servizio e dalla retribuzione fino ad un massimo di dieci giorni** il dipendente che nel violare i protocolli interni previsti dal presente Modello 231 o adottando nell'espletamento di attività nelle Processi/Aree a rischio un comportamento in violazione delle prescrizioni dello stesso, arrechi danno a CSI o la esponga a una situazione oggettiva di pericolo alla integrità dei beni della stessa,

- purché tali condotte non siano comunque dirette in modo univoco alla commissione del Reato o non determinino l'applicazione di misure previste dal Decreto 231;
3. incorre nel provvedimento di **licenziamento per giusta causa o giustificato motivo a seconda della gravità della violazione ai sensi dell'art._71 del CCNL** il dipendente che adotti un comportamento non conforme ai protocolli interni previsti dal presente Modello 231 e diretto in modo univoco al compimento di un reato sanzionato dal Decreto 231, nonché il dipendente che adotti un comportamento palesemente in violazione dei protocolli interni previsti dal presente Modello 231, tale da determinare la concreta applicazione a carico di CSI di misure previste dal Decreto 231.

Inoltre, con specifico riferimento alle violazioni delle prescrizioni del Modello previste in materia di **tutela della salute e della sicurezza sui luoghi di lavoro**:

1. incorre nel provvedimento di **sospensione dal servizio e dalla retribuzione fino ad un massimo di dieci giorni** il dipendente che, nel violare i protocolli interni previsti dal presente Modello in materia di tutela della salute e della sicurezza sui luoghi di lavoro, abbia adottato un comportamento in violazione alle prescrizioni del Modello stesso ingenerando un rilevante rischio differenziale⁵ tale da esporre CSI ad un più grave rischio di applicazione di misure previste dal Decreto 231 (trattasi, ad esempio, della condotta negligente, imperita od imprudente del lavoratore durante le attività di formazione e addestramento);
2. incorre nel provvedimento del **licenziamento per giustificato motivo o giusta causa a seconda della gravità della violazione ai sensi dell'art._71 del CCNL** il lavoratore che adotti un comportamento in violazione dei protocolli interni previsti dal presente Modello 231 tale da esporre CSI al rischio concreto ed immediato di applicazione di misure previste dal Decreto 231 (trattasi, a mero titolo esemplificativo, della condotta negligente, imprudente od imperita suscettibile di provocare un infortunio a sé stesso ovvero ad altre persone).

7.3 Violazioni del Modello 231 da parte dei dirigenti e relative misure

Per quanto attiene alle violazioni delle singole regole di cui al presente Modello 231, poste in essere dai dirigenti di CSI, anche queste costituiscono illecito disciplinare.

Qualsiasi tipo di violazione delle regole contenute nel Modello 231 autorizza l'OdV a richiedere alle funzioni aziendali competenti di CSI l'irrogazione di una delle sanzioni di seguito elencate e determinata sulla base della gravità della violazione commessa alla luce dei criteri indicati nel paragrafo 6.1 e del comportamento tenuto prima (e.g. eventuali precedenti violazioni commesse) e dopo il fatto (e.g. comunicazione all'OdV dell'avvenuta irregolarità) dall'autore della violazione.

I provvedimenti disciplinari irrogabili nei riguardi dei dirigenti - nel rispetto delle procedure previste dall'articolo 7 della Legge 30 maggio 1970, n. 300 (Statuto dei Lavoratori), delle eventuali normative speciali applicabili, e del CCNL Dirigenti Dipendenti dalle Imprese creditizie, finanziarie e strumentali (19 aprile 2005, rinnovato il 10 gennaio 2008 e il 29 febbraio 2012) sono le seguenti:

- a) censura scritta;
- b) sospensione disciplinare;

⁵ Con specifico riferimento alle violazioni a prescrizioni del Modello 231 previste in materia di tutela della salute e della sicurezza sui luoghi di lavoro, si precisa che per "rischio differenziale" si deve intendere il margine di rischio ulteriore rispetto a quello già individuato in sede di valutazione dei rischi da parte di CSI e derivante dal comportamento del lavoratore.

- c) licenziamento per giustificato motivo;
- d) licenziamento per giusta causa.

In ogni caso, delle sanzioni irrogate e/o delle violazioni accertate, la funzione aziendale competente terrà sempre informato l'OdV.

In particolare, con riferimento alle violazioni del Modello 231 poste in essere dai dirigenti di CSI, si prevede che:

- in caso di violazione non grave di uno o più protocolli interni, regole procedurali o comportamentali previste nel Modello, il dirigente incorre nella **censura scritta** consistente nel richiamo all'osservanza del Modello 231, la quale costituisce condizione necessaria per il mantenimento del rapporto fiduciario con CSI;
- in caso di violazione non grave, ma reiterata, di uno o più protocolli interni, regole procedurali o comportamentali previste nel Modello 231, il dirigente incorre nel provvedimento della **sospensione disciplinare**;
- in caso di grave violazione di uno o più protocolli interni, regole procedurali o comportamentali previste nel Modello 231 tale da configurare un notevole inadempimento, il dirigente incorre nel provvedimento del **licenziamento per giustificato motivo**;
- laddove la violazione di uno o più protocolli interni, regole procedurali o comportamentali previste nel Modello sia di gravità tale da ledere irreparabilmente il rapporto di fiducia, non consentendo la prosecuzione anche provvisoria del rapporto di lavoro, il dirigente incorre nel provvedimento del **licenziamento per giusta causa**.

Inoltre, per i lavoratori di CSI aventi qualifica di 'dirigente' costituisce grave violazione delle prescrizioni del Modello 231:

- l'inosservanza dell'obbligo di direzione o vigilanza sui lavoratori subordinati circa la corretta ed effettiva applicazione del Modello 231 stesso.
- l'inosservanza dell'obbligo di direzione e vigilanza sugli altri lavoratori che, sebbene non legati a CSI da un vincolo di subordinazione (trattasi, ad esempio, di lavoratori autonomi, agenti, consulenti, collaboratori coordinati e continuativi ecc.), sono comunque soggetti alla direzione e vigilanza del 'Dirigente' ai sensi dell'art. 5 comma 1 lett. b) del D.lgs. 231/01.

7.4 Misure nei confronti dei Consulenti, Collaboratori, Appaltatori, promotori finanziari o "Personal Banker"

Ogni violazione posta in essere dai Consulenti, Collaboratori (ivi compresi i lavoratori somministrati e i lavoratori a progetto), Appaltatori e promotori finanziari ("Personal Banker"), potrà determinare, secondo quanto previsto dalle specifiche clausole contrattuali inserite nelle lettere di incarico o negli accordi di collaborazione, la risoluzione del rapporto contrattuale, fatta salva l'eventuale richiesta di risarcimento, qualora da tale comportamento derivino danni a CSI, come nel caso di applicazione da parte del giudice delle misure previste dal Decreto 231.

7.5 Misure nei confronti di componenti del CdA, del collegio sindacale e dell'OdV

In caso di violazione del Modello da parte di uno o più componenti del Consiglio di Amministrazione di CSI, l'OdV informerà l'intero Consiglio di Amministrazione e il Collegio Sindacale, che prenderanno gli opportuni provvedimenti coerentemente con la gravità della violazione commessa alla luce dei criteri indicati nel paragrafo 6.1 e conformemente ai poteri previsti dalla legge e/o dallo Statuto (dichiarazioni nei verbali delle adunanze, richiesta di

convocazione o convocazione dell'Assemblea con all'ordine del giorno adeguati provvedimenti nei confronti dei soggetti responsabili della violazione ecc.).

I provvedimenti irrogabili nei riguardi di uno o più membri del Consiglio di Amministrazione di CSI, previa delibera del Consiglio di Amministrazione da adottare con l'astensione dell'interessato e, ove previsto dalla legge e/o dallo Statuto, con delibera dell'Assemblea dei soci, sono quelli previsti dal seguente apparato sanzionatorio:

- a) richiamo scritto;
- b) sospensione temporanea dalla carica;
- c) revoca dalla carica.

In particolare, con riferimento alle violazioni del Modello 231 poste in essere da uno o più componenti del Consiglio di Amministrazione di CSI, si prevede che:

- in caso di violazione non grave di una o più regole procedurali o comportamentali previste nel Modello 231, il componente del Consiglio di Amministrazione incorra nel **richiamo scritto** consistente nel richiamo all'osservanza del Modello, la quale costituisce condizione necessaria per il mantenimento del rapporto fiduciario con CSI;
- laddove la violazione di una o più prescrizioni del Modello 231 sia di gravità tale da ledere irreparabilmente il rapporto di fiducia, non consentendo la prosecuzione anche provvisoria del rapporto, il componente del Consiglio di Amministrazione incorre nella **decadenza/revoca dalla carica**.

Inoltre, per i componenti del Consiglio di Amministrazione di CSI, costituirà violazione del Modello 231 sanzionabile anche la violazione dell'obbligo di direzione o vigilanza sui sottoposti circa la corretta e l'effettiva applicazione delle prescrizioni del Modello 231.

In caso di violazione del Modello 231 da parte di uno o più membri del Consiglio di Amministrazione di CSI, l'OdV informerà il Consiglio di Amministrazione stesso il quale provvederà ad assumere le iniziative ritenute più più idonee.

In caso di violazione del Modello 231 da parte dell'intero Consiglio di Amministrazione di CSI, l'OdV informerà il Collegio Sindacale affinché questo convochi senza indugio l'Assemblea dei Soci per gli opportuni provvedimenti.

In caso di violazione del Modello 231 da parte di uno o più membri del Collegio Sindacale di CSI, l'OdV informerà il Consiglio di Amministrazione, i quali prenderanno gli opportuni provvedimenti coerentemente con la gravità della violazione e conformemente ai poteri previsti dalla legge e/o dallo Statuto (dichiarazioni nei verbali delle adunanze, richiesta di convocazione o convocazione dell'Assemblea con all'ordine del giorno adeguati provvedimenti nei confronti dei soggetti responsabili della violazione ecc.)

Qualora il CdA fosse informato in merito a violazioni del Modello 231 da parte di uno o più membri dell'OdV, il detto CdA provvederà ad assumere le iniziative ritenute più idonee coerentemente con la gravità della violazione e conformemente ai poteri previsti dalla legge e/o dallo Statuto.

In particolare, qualora la violazione sia commessa da un componente dell'OdV che sia anche un dipendente o dirigente di CSI si applicheranno le sanzioni di cui ai Paragrafi 6.2 e 6.3 della Parte Generale del Modello.

PARTE SPECIALE**8 REATI NEI CONFRONTI DELLA PUBBLICA AMMINISTRAZIONE****8.1 Le fattispecie di reato**

Le fattispecie di reato nei confronti della Pubblica Amministrazione, contemplate agli artt. 24 e 25 del D.Lgs. 231/01, comprendono:

Art. 24 – Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico

- **Malversazione a danno dello Stato (Art. 316-bis c.p.)** – Presupposto del reato in esame è l'avvenuta erogazione da parte di un ente pubblico in favore di un soggetto attivo di una somma per la realizzazione di opere di interesse pubblico. Ai sensi dell'art. 316 bis c.p. risponde a tale reato chiunque, estraneo alla Pubblica Amministrazione, avendo ottenuto dallo Stato, da un altro ente pubblico o dalla Comunità Europea contributi, sovvenzioni o finanziamenti per la realizzazione di opere o per lo svolgimento di attività di pubblico interesse, non li destina a dette attività
- **Indebita percezione di erogazioni a danno dello Stato (Art. 316-ter c.p.)** – Presupposto del reato è che l'erogazione pubblica sia conseguita a mezzo dell'esibizione di documentazione falsa ovvero per l'omissione di informazioni dovute. La Società sarà chiamata a rispondere in sede penale ove la condotta illecita sia stata posta in essere dai suoi funzionari, in tal modo assicurando all'istituto un finanziamento al quale non avrebbe diritto
- **Truffa a danno dello Stato o di altro ente pubblico (art. 640 c.p.)** – Tale ipotesi di reato si realizza qualora un dipendente o rappresentante della Banca, attraverso artifici o raggiri (es, esibendo documenti falsi), induca lo Stato o un ente pubblico in errore, ricavandone un profitto cagionando un danno allo Stato o all'ente pubblico
- **Truffa aggravata per il conseguimento di erogazioni pubbliche (Art. 640-bis c.p.)** - Presupposto del reato è che la truffa riguardi l'erogazione di contributi, finanziamenti, mutui agevolati ed altre erogazioni concesse da parte dello Stato, di enti pubblici o della Comunità Europea. Si rinvia a quanto osservato nei casi previsti agli artt. 316-ter e 640 del c.p.. Si pensi ad esempio a truffe perpetuate ai danni di enti previdenziali, ovvero amministrazioni locali o ripartizioni di queste, attraverso dichiarazioni mendaci o altre condotte fraudolente.
- **Frode informatica se commessa in danno dello Stato o di altro ente pubblico (Art. 640-ter c.p.)** – Tale ipotesi di reato si configura nel caso di alterazione del funzionamento di un sistema informatico o telematico o di intervento senza diritto su dati, informazioni, programmi allo scopo di trarne profitto con danno d'altri. Ad esempio è configurabile nel caso in cui, attraverso l'alterazione del software di controllo INPS per le denunce retributive, si ottenga un ingiusto vantaggio con danno dell'ente previdenziale.

Art. 25 - Concussione e Corruzione

- **Concussione (art. 317 c.p.)** – Commette tale reato il pubblico ufficiale o l'incaricato di pubblico servizio che, abusando delle sua qualità o dei suoi poteri, costringe o induce taluno a dare a o promettere indebitamente, a lui o ad un terzo, denaro o altra utilità. E' ipotizzabile la commissione del reato in ambito bancario ad esempio nel caso in cui la banca gestisca, in regime di concessione o sotto altra forma, un pubblico servizio oppure nel

caso in cui il soggetto, che agisce in nome e per conto della banca, agevoli o istighi un pubblico ufficiale o un incaricato di pubblico servizio alla concussione, assumendo così la qualifica di concorrente nel reato.

- **Corruzione per l'esercizio della funzione (art. 318 c.p.) –Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.)** – Tale ipotesi di reato si configura nel caso in cui un rappresentante o dipendente della Banca dia o prometta a un Pubblico Ufficiale, per sé o per altri, denaro o altra utilità (es. doni in natura) per omettere o ritardare, per avere omesso o ritardato, un atto del suo ufficio, ovvero per compiere o per avere compiuto un atto contrario ai doveri di ufficio. Il reato si configura sia nei confronti del corrotto che del corruttore.
- **Corruzione in atti giudiziari (art. 319 ter c.p.)** – Si caratterizza rispetto ai reati precedenti sotto il profilo del dolo specifico. Tale ipotesi di reato si verifica qualora il dipendente o rappresentante della Banca corrompa un magistrato o un testimone al fine di ottenere favori in un procedimento civile, penale o amministrativo che vede coinvolta la stessa società o un soggetto terzo.
- **Induzione indebita a dare o promettere utilità (art. 319-quater c.p.)** - Tale ipotesi di reato si configura nel caso in cui il pubblico ufficiale o l'incaricato di pubblico servizio, abusando della sua qualità o dei suoi poteri, induca taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità. Il reato si configura nei confronti anche dell'indotto.
- **Corruzione di persona incaricata di pubblico servizio (art. 320 c.p.)** – Tale ipotesi di reato si configura nel caso in cui la corruzione per un atto d'ufficio o per un atto contrario ai doveri di ufficio riguardino un Incaricato di Pubblico Servizio.
- **Istigazione alla corruzione (art. 322 c.p.)** - Tale ipotesi di reato si configura nel caso in cui il dipendente o rappresentante della Banca offra denaro o altra utilità a un Pubblico Ufficiale o ad un Incaricato di Pubblico Servizio per una finalità corruttiva ma l'offerta o la promessa non sia accettata.
- **Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte Penale internazionale o degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri**– Tale ipotesi di reato si configura nel caso in cui un dipendente o rappresentante della Banca commetta i delitti di peculato, concussione, induzione indebita a dare o promettere utilità e istigazione alla corruzione con riguardo ai membri delle istituzioni comunitarie (Commissione Europea, Parlamento Europeo, Corte di Giustizia, Corte dei Conti).

8.2 Nozione di “Pubblico Ufficiale” e “Incaricato di Pubblico Servizio”

Ai sensi degli artt. 357 e 358 c.p., sono pubblici ufficiali ed incaricati di pubblico servizio tutti coloro che – legati o meno da un rapporto di dipendenza con la P.A. – svolgono un'attività regolata da norme di diritto pubblico. In particolare:

- pubblico ufficiale è colui che esercita una pubblica funzione legislativa, giudiziaria o amministrativa; tale funzione è caratterizzata dalla formazione e dalla manifestazione di volontà della pubblica amministrazione e dal suo svolgersi per mezzo di poteri autorizzativi o certificativi;
- incaricato di pubblico servizio è colui che, come il pubblico ufficiale svolge una pubblica funzione ma a differenza di quest'ultimo, non ha potestà di imperio e di certificazione documentale.

La nozione di pubblico ufficiale o incaricato di pubblico servizio ha, dunque, natura oggettiva, basandosi sull'attività concretamente svolta dal soggetto e non sull'esistenza di un rapporto – contrattuale o di dipendenza – con la P.A.: è conseguentemente possibile che soggetti, la cui attività è di regola disciplinata dal diritto privato, in taluni settori operino in qualità di pubblici agenti. Per quanto riguarda l'attività bancaria ordinaria, non vi sono dubbi riguardo alla sua natura privatistica enunciata dal Testo Unico Bancario, che all'art. 10 recita *“la raccolta del risparmio tra il pubblico e l'esercizio del credito costituiscono l'attività bancaria. Essa ha carattere di impresa”*.

Occorre tuttavia precisare che ancorché la natura privatistica dell'attività bancaria sia ormai un dato acquisito al nostro ordinamento, vi possono essere delle attività che esulano dalla gestione ordinaria del credito e che, in quanto svolte in regime di concessione, potrebbero presentare connotazioni pubblicistiche.

Tali potrebbero essere, secondo l'elaborazione giurisprudenziale:

- le operazioni che attengono all'attività di intermediazione bancaria consistente nella distribuzione di titoli del debito pubblico;
- le operazioni svolte in campo monetario, valutario, fiscale e finanziario, in sostituzione di enti pubblici, nella veste di banche agenti o delegate;
- le operazioni relative alle attività di concessione e gestione di “crediti di scopo legale” e a quelle rientranti nel settore dei c.d. “crediti speciali agevolati” che, per loro natura, gravano in varia misura sulla finanza pubblica.

Ciò premesso, deve tuttavia escludersi che la Banca svolga attualmente alcuna attività in regime di pubblica concessione o riconducibile in qualsiasi modo allo svolgimento di una pubblica funzione.

Si precisa infine che, ai pubblici agenti italiani sono equiparati tutti coloro che svolgono funzioni analoghe a quelle che ad essi competono nell'ambito di organismi comunitari, di altri Stati membri dell'Unione europea, di Stati esteri o organizzazioni pubbliche internazionali.

8.3 Processi/Aree a rischio

Nella tabella di sintesi sono indicate le aree individuate come sensibili alla commissione delle fattispecie di reato nei confronti della Pubblica Amministrazione.

	Direzione Executive Board Collegio Sindacale	Regional Management (BPPM e ORM)	PB: Canali distribuiti	Corporate Advisory	Advisory and Sales (AOF, Product and Services, Investment Consulting)	PB: FOS Casse	CP&D	AM: Canali distribuiti	AM: Portfolio Management and Product Control	Internal Audit	Direttore Compliance	Direttore Legal	Operations	Information Technology	Credit Manager	CRES - Immobili Servizi/Sicurezza e Prevenzione	Direttore Ufficio Acquisti - Supply Mgmt	Direttore Risorse Umane	Direttore Financial Accounting
REATI CONTRO LA PUBBLICA AMMINISTRAZIONE	Malversazione a danno dello Stato o di altro ente pubblico	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	SI	NO
	Indebita percezione di contributi, finanziamenti o altre erogazioni da parte dello Stato o di altro ente pubblico	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	SI	NO
	Truffa in danno dello Stato o di altro ente pubblico	SI	NO	SI	SI	NO	NO	SI	SI	NO	NO	NO	NO	NO	NO	NO	NO	SI	NO
	Truffa aggravata per il conseguimento di erogazioni pubbliche	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	SI	NO
	Frode informatica in danno dello Stato o di altro ente pubblico	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	SI	NO	NO	NO	NO	NO
	Corruzione per un atto d'ufficio	SI	NO	SI	SI	NO	NO	SI	NO	NO	SI	SI	NO	NO	NO	SI	SI	SI	SI
	Corruzione per un atto contrario ai doveri d'ufficio	SI	NO	SI	SI	NO	NO	SI	NO	NO	SI	SI	NO	NO	NO	SI	SI	SI	SI
	Corruzione di persona incaricata di un pubblico servizio	SI	SI	SI	SI	NO	NO	SI	NO	NO	SI	SI	NO	NO	NO	SI	SI	SI	SI
	Corruzione in atti giudiziari	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	SI	NO	NO	NO	NO	NO	NO	NO
	Istigazione alla corruzione	SI	NO	SI	SI	NO	NO	SI	NO	NO	SI	SI	NO	NO	NO	SI	SI	SI	SI
	Peculato, concussione, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	SI	SI	NO
	Concussione	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO

8.4 Principi di controllo e di comportamento ed assetto del sistema di organizzazione, gestione e controllo

La presente sezione illustra le regole di condotta e di comportamento, nonché di assetto del sistema di organizzazione, gestione e controllo che, dovranno essere seguite dai Destinatari al fine di prevenire il verificarsi dei Reati descritti al precedente Paragrafo 8.1.

All'uopo è fatto **divieto** in particolare di:

- compiere azioni o tenere comportamenti che siano o possano essere interpretati come pratiche di corruzione, favori illegittimi, comportamenti collusivi, sollecitazioni, dirette o mediante terzi, di privilegi per sé o per altri rilevanti ai fini della commissione dei reati di cui al Decreto;
- adottare comportamenti contrari alle Leggi, al Codice di Condotta e, più in generale, a quanto definito nell'ambito del Regolamento di Direzione (di cui il Codice di Condotta e il presente Modello 231 sono parte integrante), al Mansionario, alle Direttive emate dal Gruppo, alle Procedure aziendali, al Documento Programmatico sulla Sicurezza, in sede di ispezioni/controlli/verifiche da parte degli Organismi pubblici o nominati dall'Organo giudicante, anche a mezzo di professionisti esterni, per influenzarne il giudizio/parere nell'interesse della Banca;
- adottare comportamenti contrari alle Leggi, al Codice di Condotta e, più in generale, a quanto definito nell'ambito del Regolamento di Direzione (di cui il Codice di Condotta e il presente Modello 231 sono parte integrante), al Mansionario, alle Direttive emate dal Gruppo, alle Procedure aziendali, al Documento Programmatico sulla Sicurezza, in sede di decisione del contenzioso/arbitrato, anche a mezzo di professionisti esterni, per influenzare indebitamente le decisioni dell'Organo giudicante o le posizioni della Pubblica Amministrazione quando questa sia controparte del contenzioso;
- distribuire o ricevere omaggi e regali al di fuori di quanto previsto dal Codice di Condotta, dalle Direttive emanate dal Gruppo, dalle Procedure aziendali (vale a dire ogni forma di regalo offerto o ricevuto, allo scopo di influenzare il destinatario nell'espletamento dei suoi doveri e/o allo scopo di trarre indebito vantaggio, o che possa anche solo essere interpretato come eccedente le normali pratiche commerciali o di cortesia, o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale) e dal presente Modello 231. In particolare, non è consentito offrire denaro o utilità di qualsiasi tipo (promesse di assunzione, ecc.) o compiere atti di cortesia commerciale in favore di esponenti della Pubblica Amministrazione italiana ed estera (anche in quei paesi in cui l'elargizione di doni rappresenta una prassi diffusa), o loro parenti, salvo che si tratti di utilità di modico valore ed elargite nel rispetto delle procedure aziendali e sempre che comunque non possano essere in alcun modo interpretate quale strumento per influenzarli nell'espletamento dei loro doveri (sia affinché agiscano in un dato senso od omettano di agire), per ricevere favori illegittimi e/o per trarne indebito. I regali offerti - salvo quelli di modico valore - devono essere documentati in modo adeguato per consentire le prescritte verifiche;
- esercitare indebite pressioni o sollecitazioni su pubblici agenti in vista del compimento di attività inerenti l'ufficio;
- presentare dichiarazioni non veritiere a organismi pubblici nazionali, ed esteri al fine di conseguire autorizzazioni, licenze e provvedimenti amministrativi di qualsivoglia natura;
- esibire documenti e dati incompleti e/o comunicare dati falsi o alterati;
- tenere una condotta ingannevole che possa indurre le Autorità di Vigilanza o gli Enti pubblici in errore in ordine alla scelta di attribuzione di incarichi alla Banca;
- chiedere o indurre i rappresentanti dell'autorità di vigilanza a trattamenti di favore ovvero omettere informazioni dovute al fine ostacolare l'esercizio delle funzioni di vigilanza
- effettuare o promettere, in favore dei clienti, prestazioni che non trovino adeguata giustificazione alla luce del rapporto contrattuale con essi costituito onde evitare di costituire fondi utilizzabili per la commissione di uno dei reati;

- assegnare incarichi di fornitura ed incarichi professionali in assenza di autorizzazioni alla spesa e dei necessari requisiti di professionalità, qualità e convenienza del bene o servizio fornito;
- procedere all'attestazione di regolarità in fase di ricezione di beni/servizi in assenza di un'attenta valutazione di merito e di congruità in relazione al bene/servizio ricevuto;
- procedere all'autorizzazione al pagamento di beni/servizi in assenza di una verifica circa la congruità della fornitura/prestazione rispetto ai termini contrattuali;
- procedere all'autorizzazione del pagamento di parcelle in assenza di un'attenta valutazione del corrispettivo in relazione alla qualità del servizio ricevuto;
- effettuare pagamenti in favore di fornitori della Banca che non trovino adeguata giustificazione nel contesto del rapporto contrattuale in essere con gli stessi onde evitare di costituire fondi utilizzabili per la commissione di uno dei reati;
- riconoscere, in favore degli Appaltatori, dei Consulenti e dei promotori finanziari (Personal Banker), compensi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alla prassi vigente nel settore di attività interessato;
- concludere contratti di consulenza con soggetti interni alla Pubblica Amministrazione in base ai quali si potrebbe minare l'imparzialità e il buon andamento della Pubblica Amministrazione stessa;
- affidare incarichi a eventuali consulenti esterni eludendo criteri documentabili ed obiettivi incentrati su competitività, utilità, prezzo, integrità, solidità e capacità di garantire un'efficace assistenza continuativa. In particolare, le regole per la scelta del consulente devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice di Condotta e, più in generale, da quanto definito nell'ambito del Regolamento di Direzione (di cui il Codice di Condotta e il presente Modello 231 sono parte integrante), dalle Direttive e alle Procedure aziendali; ciò al fine di prevenire il rischio di commissione di reati di corruzione che potrebbe derivare dall'eventuale scelta di soggetti "vicini" a persone legate alla Pubblica Amministrazione e alla conseguente possibilità di agevolare l'instaurazione/sviluppo di rapporti finalizzati alla stipula;
- chiedere o indurre i soggetti della Pubblica Amministrazione a trattamenti di favore ovvero omettere informazioni dovute al fine di influenzare impropriamente la decisione di stipulare accordi/convenzioni/contratti con la Banca;
- promettere o versare/offrire somme di denaro, doni o gratuite prestazioni al di fuori di quanto previsto dalla prassi aziendale o dalla prassi del contesto in cui si opera (ad esempio festività, usi e costumi locali, di mercato o commerciali) e accordare vantaggi di qualsiasi natura a rappresentanti della Pubblica Amministrazione a titolo personale con la finalità di promuovere o favorire interessi della Banca. Tra i vantaggi che potrebbero essere accordati, si citano, a titolo esemplificativo ancorché non esaustivo, la promessa di assunzione per parenti ed affini e, a titolo più generale, tutte le operazioni bancarie o finanziarie che comportino la generazione di una perdita per la Banca e la creazione di un utile per il pubblico ufficiale (es. stralcio di posizione debitoria e/o applicazioni di condizioni non in linea con i parametri di mercato)
- alterare il **funzionamento di un sistema informatico o telematico** ovvero di intervenire senza diritto sui dati, informazioni o programmi contenuti nel sistema di scambio di dati con le Autorità di Vigilanza;

Ai fini dell'attuazione dei divieti suddetti, dovranno rispettarsi le **regole** di seguito indicate:

- i rapporti con la Pubblica Amministrazione devono avvenire nell'assoluto rispetto delle leggi, delle normative vigenti, dei principi di lealtà e correttezza, nonché dei principi contenuti nel Modello 231 e nel Regolamento di Direzione e delle indicazioni contenute nel Mansionario, nelle Direttive emanate dal Gruppo e nelle Procedure aziendali, in qualunque fase di gestione del rapporto;

- tutti coloro che materialmente intrattengono rapporti con la P.A. per conto della Banca devono essere in possesso di apposita autorizzazione da parte della Banca. Tali soggetti devono, inoltre, ispirarsi ai principi di trasparenza e correttezza nel trattare con la P.A.
- la gestione delle attività svolte nell'ambito delle Aree/Processi a Rischio dovrà avvenire esclusivamente ad opera delle funzioni/soggetti aziendali competenti;
- le attività svolte nell'ambito delle Aree/Processi a Rischio devono essere disciplinate in modo da dettagliare ogni fase del processo, evidenziare le attività svolte, i controlli/le verifiche eseguiti e il processo autorizzativo; identificare in maniera chiara i soggetti e le funzioni che svolgono le varie attività (attività operative-gestionali, attività di controllo, attività di autorizzazione/approvazione); definire le modalità e la responsabilità per la documentazione e la tracciabilità delle singole attività svolte;
- il sistema dei poteri e delle deleghe stabilisce le facoltà di autonomia gestionale per natura di spesa ed impegno, ivi inclusi quelli nei confronti della Pubblica Amministrazione; la normativa interna illustra i predetti meccanismi autorizzativi, fornendo l'indicazione dei soggetti aziendali cui sono attribuiti i necessari poteri;
- il sistema dei poteri e delle deleghe stabilisce la chiara attribuzione dei poteri relativi alla definizione delle transazioni;
- tutte le erogazioni di fondi devono essere approvate dai soggetti facoltizzati in base al vigente sistema dei poteri e delle deleghe;
- il budget della Banca è predisposto e approvato dal *Consiglio di Amministrazione*;
- e' necessario mantenere una segregazione dei compiti tra i differenti soggetti coinvolti nei vari processi sensibili finalizzati ad intrattenere rapporti con gli Enti Pubblici, in particolare:
 - con riferimento alla gestione dei rapporti non riconducibili alla ordinaria operatività delle Unità Organizzative della Banca, tutta la corrispondenza inerente a rilievi o eccezioni relative alla sfera dell'operatività aziendale indirizzata alle Autorità di Vigilanza è preventivamente condivisa con le competenti Funzioni Compliance e Legal;
 - le attività di cui alle diverse fasi dei Processi a Rischio devono essere svolte da soggetti differenti chiaramente identificabili;
- i processi sia a livello informativo sia in termini documentali devono essere tracciabili, in particolare:
 - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, ciascuna Unità Organizzativa è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica, nonché degli accordi/convenzioni/contratti definitivi, nell'ambito delle attività proprie del processo della stipula di rapporti con la Pubblica Amministrazione;
 - completa tracciabilità a livello documentale e di sistema dei processi di gestione degli omaggi, delle spese di rappresentanza, delle beneficenze e sponsorizzazioni anche attraverso la redazione, da parte di tutte le Unità Organizzative interessate, di una reportistica sulle erogazioni effettuate/contratti stipulati;
- il personale non può dare seguito e deve immediatamente segnalare per le azioni del caso al proprio Responsabile qualunque richiesta di indebiti vantaggi o tentativi di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente venire a conoscenza; il Responsabile a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta all'Organismo di Vigilanza per le valutazioni del caso;
- i soggetti e le funzioni coinvolte nelle Aree/Processi a Rischio devono osservare scrupolosamente le indicazioni contenute nelle specifiche a disciplina delle attività svolte nei processi stessi;
- tutti coloro che materialmente intrattengono rapporti con la Pubblica Amministrazione per conto di CSI (ivi inclusi i rapporti intrattenuti in occasione di effettuazione di verifiche ispettive o sopralluoghi) devono godere di un'autorizzazione in tal senso da parte CSI stessa, consistente in un'apposita delega o direttive organizzative interne per i dipendenti, i collaboratori (ivi compresi i lavoratori somministrati e i lavoratori a progetto), i promotori

finanziari (Personal Banker) e gli organi sociali ovvero in un contratto di fornitura/consulenza o di collaborazione opportunamente formalizzato;

- il sistema dei poteri e delle deleghe stabilisce le facoltà di autonomia gestionale per natura di spesa ed impegno, anche con riferimento a quelli nei confronti della Pubblica Amministrazione;
- tutti i soggetti che intervengono nella fase di gestione dei rapporti pre-contrattuali con la Pubblica Amministrazione devono essere individuati e autorizzati tramite delega interna;
- tutti i dipendenti della Banca, i collaboratori (ivi compresi i lavoratori somministrati e i lavoratori a progetto) e i promotori finanziari (Personal Banker) dovranno attenersi scrupolosamente e rispettare eventuali limiti previsti nelle deleghe organizzative o procure conferite da CSI;
- i Destinatari non possono effettuare o promettere, in favore dei terzi, prestazioni che non trovino adeguata giustificazione alla luce del rapporto contrattuale con essi instaurato o che non siano debitamente formalizzate in un contratto o in un accordo, ad es. con la finalità di influenzare il giudizio del pubblico funzionario nel caso di verifiche ispettive;
- i prodotti e/o servizi acquistati devono essere giustificati da concrete esigenze aziendali, motivate e risultanti da evidenze interne quanto a finalità dell'acquisto, individuazione del richiedente e processo di autorizzazione della spesa, nei limiti del budget disponibile e comunque in accordo alle Direttive e Procedure aziendali;
- in particolare, l'approvazione della richiesta di acquisto, il conferimento dell'incarico, il perfezionamento del contratto e l'emissione dell'ordine spettano esclusivamente a soggetti muniti di idonee facoltà in base al sistema di poteri e deleghe in essere che stabilisce le facoltà di autonomia gestionale per natura di spesa e impegno. Le procedure Direttive e Procedure aziendali illustrano i predetti meccanismi autorizzativi, fornendo l'indicazione dei soggetti aziendali cui sono attribuiti i necessari poteri;
- è altresì fatto divieto di procedere all'attestazione di regolarità in fase di ricezione di beni/servizi in assenza di un'attenta valutazione di merito e di congruità in relazione al bene/servizio ricevuto e di procedere all'autorizzazione al pagamento di beni/servizi in assenza di una verifica circa la congruità della fornitura/prestazione rispetto ai termini contrattuali;
- nessun tipo di pagamento non adeguatamente documentato ed autorizzato può esser effettuato;
- sono definiti diversi profili di utenza per l'accesso a procedure informatiche ai quali corrispondono specifiche abilitazioni in ragione delle funzioni attribuite;
- la Banca può effettuare erogazioni sotto forma di beneficenze o sponsorizzazioni per sostenere iniziative di Enti regolarmente costituiti ai sensi di legge e che promuovono i principi etici conformi a quelli della Banca;
- eventuali iniziative la cui classificazione rientri nei casi previsti per le "sponsorizzazioni" non possono essere oggetto contemporaneo di erogazione per beneficenza;
- per quanto attiene gli omaggi e le spese di rappresentanza destinati, seppure in modo non esclusivo, ad esponenti della Pubblica Amministrazione, le Direttive e Procedure aziendali stabiliscono idonei limiti quantitativi rapportati al valore di tali omaggi/spese (policy GP-00289 Regali e intrattenimenti);
- per le sponsorizzazioni è necessaria una puntuale verifica del corretto adempimento della controprestazione acquisendo idonea documentazione comprovante l'avvenuta esecuzione della stessa;
- i responsabili delle Unità Organizzative interessate devono disporre che venga regolarmente tenuto in evidenza l'elenco dei beneficiari, l'importo delle erogazioni ovvero gli omaggi distribuiti nonché le relative date/occasioni di elargizioni. Tali obblighi non si applicano per gli omaggi cosiddetti "marchiati", riportanti il Logotipo della Banca (quali biro, oggetti da scrivania, ecc...);
- è fatto obbligo ai soggetti incaricati di registrare e documentare i rapporti tra le singole funzioni aziendali e i Pubblici Ufficiali e/o gli Incaricati di Pubblico Servizio. Detta

documentazione può essere oggetto di verifica da parte dei responsabili delle funzioni aziendali cui il soggetto appartiene e in ogni caso deve essere comunicata da questi ultimi all'OdV, secondo quanto stabilito nella Parte Generale;

- i responsabili delle funzioni della Banca coinvolti nelle Aree a Rischio devono garantire il costante aggiornamento e sensibilizzazione del personale e dei terzi coinvolti Aree a Rischio circa i contenuti del Modello e sulla normativa di riferimento per lo svolgimento della attività con soggetti appartenenti alla Pubblica Amministrazione;
- eventuali situazioni di incertezza in ordine ai comportamenti da tenere (anche in ragione dell'eventuale condotta illecita o semplicemente scorretta del Pubblico Ufficiale), all'interpretazione della normativa vigente e delle procedure interne devono essere sottoposte all'attenzione del superiore gerarchico e/o dell'OdV;
- l'OdV dovrà essere inoltre informato per iscritto di qualsivoglia elemento di criticità/irregolarità dovesse insorgere nell'ambito del rapporto con la Pubblica Amministrazione.

8.5 Procedure Specifiche

Ad integrazione delle regole di comportamento generali, devono rispettarsi le procedure specifiche di seguito descritte per le singole aree a rischio, nonché le ulteriori procedure di volta in volta adottate dalla Banca:

8.5.1 Gestione dei rapporti con autorità di Vigilanza e altri organismi pubblici ispettivi

a) Ispezioni e verifiche da parte di pubblici funzionari

- i rapporti con le autorità di vigilanza e con altri organismi pubblici ispettivi vanno intrattenuti dal Responsabile della succursale, dal Responsabile dell'Unità Organizzativa o da altri soggetti di riferimento appositamente incaricati tramite delega interna da conservare a cura dell'Unità Organizzativa medesima.
- non è in alcun modo consentito ai soggetti preposti e delegati a partecipare alle ispezioni di promettere od offrire a pubblici funzionari somme di denaro, regalie e qualsiasi altro bene o utilità in grado di influenzarne l'autonomia di giudizio;
- i dati ed i documenti richiesti sono consegnati in modo tempestivo, previo consenso del responsabile incaricato di interloquire con l'organo di vigilanza; i documenti consegnati devono essere completi, corretti e fornire un'esatta rappresentazione dei fatti;
- deve essere assicurata la tracciabilità di tutte le verifiche ispettive o sopralluoghi effettuati da rappresentanti della Pubblica Amministrazione mediante sottoscrizione dei verbali presentati o mediante redazione di apposita relazione interna;
- ad ogni visita ispettiva da parte di Funzionari rappresentanti delle Autorità di Vigilanza il Responsabile Unità Organizzativa interessata provvede a trasmettere all'Organismo di Vigilanza (per il tramite del Segretario) 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 Unità Organizzativa interessata dall'ispezione od un suo delegato provvede alla redazione di una nota di sintesi dell'accertamento effettuato e alla trasmissione della stessa all'Organismo di Vigilanza (per il tramite del Segretario). La suddetta documentazione è archiviata dal Responsabile dell'Unità Organizzativa interessata dall'ispezione;
- gli atti che impegnano la banca devono essere sottoscritti soltanto dai soggetti incaricati.

b) Invio periodico di dati e comunicazioni a Autorità di Vigilanza e Enti Pubblici

La procedura di invio di dati e comunicazioni sia in via telematica che attraverso altri canali deve prevedere che:

- siano effettuati dei controlli di completezza, correttezza ed accuratezza sui dati inviati agli Enti Pubblici ed alle Autorità di Vigilanza;
- i dati da trasmettere siano preventivamente controllati da una risorsa differente da quella che li ha predisposti, nel rispetto del principio di segregazione dei ruoli e delle responsabilità;
- in seguito al controllo ed alla successiva validazione dei dati, gli stessi non siano più modificabili;
- nel caso in cui l'invio dei dati avvenga in via telematica, l'accesso al sistema di trasmissione sia riservato a persone appositamente autorizzate e nel rispetto del Documento Programmatico per la Sicurezza dei Dati (DPS);
- è fatto obbligo a tutte le Unità Organizzative della Banca, a vario titolo coinvolte nella predisposizione e trasmissione di comunicazioni ed adempimenti alle Autorità di Vigilanza, di archiviare e conservare la documentazione di competenza prodotta nell'ambito della gestione dei rapporti con le Autorità, ivi inclusa quella trasmessa alle Autorità anche attraverso supporto elettronico. Tale documentazione deve essere resa disponibile a richiesta alle Funzioni Compliance e Legal e all'OdV.

8.5.2 Pagamenti a favore di Aziende ed Enti Pubblici (INPS, INAIL, Ag. Entrate ecc.)

La procedura che regola le attività di **determinazione e versamento** di importi dovuti ad Aziende ed Enti Pubblici deve prevedere che:

- le attività di conteggio, verifica, autorizzazione, disposizione di pagamento, registrazione contabile e riconciliazione siano effettuate da risorse differenti e nel rispetto del principio di segregazione funzionale;
- nel caso in cui la disposizione del pagamento (ad esempio per i contributi previdenziali) avvenga in via telematica, l'accesso al sistema di trasmissione sia riservato a persone appositamente autorizzate.

8.5.3 Gestione del contenzioso giudiziale ed extragiudiziale

La procedura che regola la gestione del **contenzioso** deve prevedere che:

- la Banca difenda i propri interessi nel rispetto dei principi sanciti nel Codice Etico e delle leggi vigenti;
- che vi sia una chiara attribuzione dei poteri relativi alla definizione delle transazioni, la facoltà di autonomia nella gestione del contenzioso incluso quello nei confronti della pubblica amministrazione;
- amministratori, i dirigenti ed i dipendenti agiscano nei limiti dei poteri e delle deleghe conferiti;
- il conferimento di incarichi a legali esterni, diversi da quelli istituzionalmente individuati, siano autorizzati dalla Direzione;
- qualora sia previsto il coinvolgimento di professionisti esterni nella gestione del contenzioso, i contratti / lettere di incarico contengano un'apposita dichiarazione di conoscenza della normativa ex D.Lgs. 231/2001 ed un impegno formale al rispetto della stessa;
- non sia possibile esercitare alcun tipo di pressione su soggetti chiamati a testimoniare di fronte all'Autorità Giudiziaria;
- la Banca non interferisca su attività investigative in corso a carico di propri amministratori, dirigenti, dipendenti, fornitori e clienti;
- in caso di accordi transattivi le Direttive e Procedure aziendali devono prevedere adeguati livelli quantitativi oltre ai quali le singole transazioni devono essere autorizzate da funzioni diverse da quelle di business che hanno gestito i rapporti con la P.A.

E' inoltre fatto specifico divieto di porre in essere comportamenti che possono rientrare nelle fattispecie di reato considerato e più in particolare di:

- elargire o promettere denaro o altre utilità a giudici, arbitri, funzionari di cancelleria, periti, testimoni ecc, come pure ai loro familiari o a coloro con i quali tali persone intrattengono notoriamente stretti legami;
- adottare comportamenti contrari alle Leggi, al Codice di Condotta e alle procedure aziendali in occasione di incontri formali ed informali e nelle fasi del procedimento, anche a mezzo di professionisti esterni e soggetti terzi, per indurre Giudici o membri di Collegi Arbitrali (compresi gli ausiliari e i periti d'ufficio) a favorire indebitamente gli interessi della banca;
- chiedere o indurre i soggetti della pubblica amministrazione a trattamenti di favore ovvero omettere informazioni dovute al fine di influenzare impropriamente la gestione del rapporto con la banca.

8.5.4. Gestione del personale.

Le procedure per la gestione del processo di selezione e assunzione del personale devono prevedere:

- la selezione del personale deve avvenire sulla base di procedure che garantiscano una valutazione dei candidati effettuata nel rispetto dei principi sanciti nel Codice di Condotta e dei seguenti principi: effettiva esigenza di nuove risorse; previa acquisizione del curriculum del candidato e svolgimento di colloqui attitudinali; omogeneità delle informazioni raccolte sui candidati mediante compilazione di apposita modulistica; valutazione comparativa sulla base di criteri obiettivi di professionalità, preparazione e attitudine in relazione alle mansioni per le quali avviene l'assunzione che sono stati definiti a priori della fase di selezione; motivazione esplicita delle ragioni poste alla base della scelta;
- devono essere previste delle disposizioni organizzative che stabiliscano in modo chiaro gli ambiti di attività dei soggetti coinvolti nel processo di selezione. La gestione del Processo a Rischio dovrà avvenire esclusivamente ad opera delle funzioni aziendali competenti, in coerenza con il sistema organizzativo. In particolare, i ruoli, i compiti e gli ambiti di attività di competenza dei soggetti coinvolti nel Processo, devono essere definiti da job description o da direttive organizzative interne che descrivano in modo esplicito il perimetro di azione e di responsabilità;
- il budget per l'assunzione di personale e i piani interni di sviluppo, ivi compresi i sistemi premianti e di incentivazione, devono essere autorizzati secondo il vigente sistema dei poteri e delle deleghe;
- l'autorizzazione all'assunzione e l'approvazione del contratto sono concesse soltanto dal personale espressamente individuato secondo il vigente sistema dei poteri e delle deleghe;
- la cessazione del rapporto lavorativo e relativi pagamenti di buona uscita sono autorizzate secondo il vigente sistema dei poteri e delle deleghe;
- il processo di selezione/assunzione del personale deve essere disciplinato in modo da dettagliare ogni fase del processo, evidenziare le attività svolte, i controlli/le verifiche eseguiti e il processo autorizzativo; identificare in maniera chiara i soggetti e le funzioni che svolgono le varie attività (attività operative-gestionali, attività di controllo, attività di autorizzazione/approvazione); definire le modalità e la responsabilità per la documentazione e la tracciabilità delle singole attività svolte;
- è fatto in particolare divieto effettuare o promettere, in favore di pubblici funzionari italiani ed esteri o a loro parenti, anche per interposta persona, proposte di assunzione tali da influenzare il giudizio del pubblico funzionario relativo alla definizione di un accordo ovvero nel corso di un rapporto CSI di qualsivoglia natura, ivi comprese le situazioni in cui tali comportamenti possano condizionare il giudizio di esponenti della Pubblica Amministrazione nel corso di ispezioni, verifiche e/o sopralluoghi.

8.5.5 Sistema degli Incentivi.

I sistemi premianti e di incentivazione devono:

- essere in grado di assicurare la coerenza con le disposizioni di legge, ed in particolare con le disposizioni della Banca d'Italia del 30 marzo 2011 in materia di "Politica e prassi di remunerazione ed incentivazione nelle banche e nei gruppi bancari", con i principi contenuti nel presente Modello 231, nonché con le previsioni del Codice di Condotta e, più in generale, del Regolamento di Direzione, anche prevedendo idonei meccanismi correttivi a fronte di eventuali comportamenti devianti;
- prevedere i criteri trasparenti di individuazione e determinazione degli incentivi, che siano strettamente correlati al conseguimento di specifici obiettivi;
- prevedere incentivi non eccessivamente "sfidanti", tali da indurre comportamenti non in linea con il Codice etico e con le previsioni del Modello 231;
- prevedere il sanzionamento di comportamenti in contrasto con il Codice di Condotta, il Modello 231 e con le procedure organizzative aziendali, determinano l'irrogazione di sanzioni consistenti nella decurtazione degli incentivi in una percentuale diversificata e commisurata al tipo di sanzione disciplinare applicata in via principale, sulla scorta del sistema previsto dalla Parte generale del Modello.

8.5.6 Gestione della formazione finanziata

La procedura di **richiesta di finanziamenti, sovvenzioni e contributi per la formazione concessi da soggetti pubblici nazionali ed esteri**, deve prevedere che:

- i rapporti con gli Enti finanziatori devono essere intrattenuti da soggetti appositamente autorizzati dalla Direzione;
- tutti i soggetti che, in fase di richiesta e gestione dei finanziamenti agevolati o contributi, intrattengono rapporti con la Pubblica Amministrazione per conto della banca devono essere espressamente incaricati ed autorizzati;
- sia verificata la coerenza dei contenuti del progetto di formazione rispetto a quanto disposto dalle direttive del bando di finanziamento;
- la documentazione inviata sia veritiera e corrispondente a quanto richiesto dall'ente erogante;
- l'invio della documentazione sia autorizzato da un legale rappresentante della Banca;
- i fondi ottenuti siano utilizzati esclusivamente per lo scopo per cui sono stati erogati;
- sia tenuto un registro relativamente all'erogazione dei progetti formativi contenente la registrazione delle presenze e delle attività svolte.

8.5.7 Gestione Acquisti e Fornitori

Le procedure devono assicurare una gestione trasparente del processo, al fine di prevenire la creazione di riserve liquide "occulte", funzionali alla commissione del reato di corruzione e devono quindi prevedere che:

- i fornitori ed i collaboratori esterni siano selezionati in base ad una procedura formalizzata e trasparente. In particolare, la selezione dei fornitori deve essere effettuata sulla base di criteri imparziali, oggettivi e documentabili e deve garantire alla Banca la migliore configurazione di costo, qualità e tempo;
- i principali fornitori devono adottare un codice etico e impegnarsi a rispettare le prescrizioni previste dal Codice di Condotta e dal Modello 231 della banca;

- non si verifichino concentrazioni di processo (individuazione dell'acquisto, selezione del fornitore, negoziazione commerciale ed emissione dell'ordine) in capo al medesimo soggetto. I soggetti incaricati per tali attività non devono esercitarla continuativamente, senza, cioè, che siano previste turnazioni idonee a coinvolgere altri soggetti, seppure appartenenti alla stessa area;
- la funzione preposta all'autorizzazione del pagamento sia diversa dalla funzione che ha firmato l'ordine di acquisto;
- siano vietati pagamenti in contanti e effettuati non a favore di conti intestati all'avente diritto (secondo quanto stabilito dagli accordi);
- sono vietati acquisti effettuati da fornitori scelti principalmente in base a criteri di amicizia, parentela o altra cointeressenza, e comunque tali da inficiare la validità in termini di prezzo e/o qualità, o che appaiano meramente strumentali alla realizzazione di una delle condotte illecite indicate nel d. lgs. 231/01;
- è vietato negoziare condizioni contrattuali occulte, che non risultano da idonea documentazione conservata unitamente a quella relativa all'acquisto.
- Vietare l'acquisto presso fornitori e consulenti segnalati da Pubblici Ufficiali

In particolare, nei rapporti con gli Enti Pubblici, devono essere osservate le seguenti previsioni:

- in caso di rapporti contrattuali con la P.A., la definizione degli accordi è esclusivamente affidata al Responsabile dell'Unità Organizzativa competente in virtù dell'oggetto del contratto o a soggetti a ciò facoltizzati;
- l'atto formale della stipula di eventuali contratti avviene in base al vigente sistema dei poteri e delle deleghe;
- ciascuna fase rilevante in caso di accordi con la Pubblica Amministrazione deve risultare da apposita documentazione scritta;
- ogni accordo/convenzione/contratto con Enti pubblici è formalizzato in un documento, debitamente firmato da soggetti muniti di idonei poteri in base al sistema dei poteri e delle deleghe in essere;
- deve essere garantita la documentabilità di ogni attività del processo con particolare riferimento alla fase di individuazione del fornitore di beni e/o servizi, o professionista anche attraverso gare, in termini di motivazione della scelta nonché pertinenza e congruità della spesa. La normativa interna individua in quali casi l'individuazione del fornitore di beni e/o servizi o professionista deve avvenire attraverso una gara o comunque tramite l'acquisizione di più offerte.

8.5.8 Gestione degli incarichi

Qualora sia previsto il coinvolgimento di soggetti terzi quali, a titolo esemplificativo Appaltatori, Consulenti, nell'ambito delle Aree/Processi a Rischio, dovranno essere rispettate le seguenti regole:

- la scelta degli Appaltatori e dei Consulenti deve avvenire sulla base di criteri di serietà e competenza del professionista/collaboratore e l'assegnazione degli incarichi deve avvenire sulla base di un processo decisionale che garantisca la segregazione dei compiti e delle responsabilità;
- gli incarichi conferiti a Consulenti e Appaltatori devono essere redatti per iscritto, con indicazione del compenso pattuito, del dettaglio della prestazione da effettuare e di eventuali deliverable attestanti l'attività svolta (nel caso in cui la prestazione lo preveda); in ogni caso non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto. Tali accordi devono essere verificati e/o approvati da soggetti dotati di adeguati poteri; tutte le dichiarazioni e le comunicazioni rese a esponenti della Pubblica Amministrazione e previste dalle norme in vigore o

specificatamente richieste dai suddetti esponenti (ad esempio in occasione di partecipazione a gare pubbliche) devono rispettare i principi di chiarezza, correttezza, completezza e trasparenza;

- le Direttive e Procedure aziendali definiscono i criteri e le casistiche in cui il coinvolgimento di soggetti terzi deve essere preventivamente sottoposto al vaglio di un'Unità Organizzativa indipendente;
- i contratti con i Consulenti devono prevedere o escludere espressamente il potere di rappresentanza di CSI nei confronti di terzi e definire in modo preciso obblighi e poteri del Consulente nello svolgimento delle attività in nome e/o per conto della Banca;
- gli ambiti di responsabilità/poteri dei Consulenti con particolare riferimento agli incarichi professionali e consulenze che comportano un rapporto diretto con la Pubblica Amministrazione, devono essere formalizzati ed espressamente richiamati nel contratto che regola il rapporto tra la Banca e tali soggetti terzi;
- gli Appaltatori, i Consulenti dovranno prendere visione del Modello e del Codice di Condotta ed impegnarsi a rispettarne le previsioni, secondo quanto stabilito in specifiche clausole, inserite nel/aggiunte al contratto stipulato tra gli stessi e la Banca, che prevedono, in ipotesi di violazione di tali previsioni, la risoluzione del suddetto contratto;
- l'attività prestata da Appaltatori e Consulenti nell'ambito delle Aree a Rischio, deve essere debitamente documentata e, comunque, la funzione che si è avvalsa della loro opera deve, prima della liquidazione dei relativi corrispettivi, attestare per iscritto l'effettività della prestazione

8.6 Controlli dell'Organismo di Vigilanza

Con riferimento alle attività a rischio, l' Organismo di Vigilanza ha facoltà discrezionale di:

- verificare che i rapporti con la Pubblica Amministrazione siano in linea con i principi sanciti nel Codice di Condotta e con le procedure aziendali;
- verificare che i rapporti con esponenti della Pubblica Amministrazione siano intrattenuti soltanto da dipendenti appositamente autorizzati;
- verificare il rispetto della segregazione funzionale nel processo di invio di dati e comunicazioni ad Aziende ed Enti Pubblici ed alle Autorità di Vigilanza;
- verificare che nel corso di ispezioni e verifiche da parte di pubblici funzionari, i soggetti autorizzati abbiano prestato un adeguato livello di collaborazione e fornito tempestivamente le informazioni ed i documenti richiesti;
- accertare che il contenzioso giudiziale ed extra giudiziale sia gestito nel rispetto della normativa vigente e delle deleghe e procure;
- controllare l'esistenza dei requisiti necessari all'ottenimento delle erogazioni pubbliche per la formazione per cui è stata fatta richiesta;
- verificare il rispetto della segregazione funzionale nel processo di pagamento a favore di Aziende ed Enti Pubblici;
- verificare la corretta applicazione delle procedure in tema di selezione dei fornitori, sponsorizzazioni, donazioni ed uscite di cassa

9 REATI SOCIETARI

9.1 Le fattispecie di reato

L'art. 3 del D.Lgs. n. 61 dell'11 aprile del 2002 ha introdotto l'art. 25 ter del D.Lgs. 231/2001, che per i reati previsti, prevede l'applicazione della sola sanzione pecuniaria, con l'esclusione delle sanzioni interdittive.

All'interno di tale fattispecie si possono prevedere i seguenti articoli del codice civile:

- **False comunicazioni sociali (art. 2621 c.c.)** – Tale ipotesi di reato si realizza se gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci, i liquidatori della Banca, con l'intenzione di ingannare i soci o il pubblico e al fine di trarre ingiusto profitto, espongono nei bilanci, relazioni o altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, fatti materiali non rispondenti al vero, ovvero omettono di fornire notizie la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della Banca o del Gruppo di appartenenza, in modo idoneo a indurre in errore i destinatari delle suddette comunicazioni.
- **False comunicazioni sociali delle società quotate (art. 2622 c.c.)** – Tale fattispecie di reato si realizza se gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società emittenti strumenti finanziari ammessi alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione europea, al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico consapevolmente espongono fatti materiali non rispondenti al vero ovvero omettono fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale la stessa appartiene, in modo concretamente idoneo ad indurre altri in errore, sono puniti con la pena della reclusione da tre a otto anni.
- **Impedito controllo (art. 2625, 2° comma c.c.)** – Tale reato si configura qualora, occultando documenti o con altri idonei artifici, gli amministratori della Banca impediscano o comunque ostacolino lo svolgimento delle attività di controllo o di revisione legalmente attribuite ai soci, al collegio sindacale o alla società di revisione cagionando un danno ai soci.
- **Indebita restituzione dei conferimenti (art. 2626 c.c.)** – Tale figura di reato si realizza nel caso in cui un amministratore della Banca, fuori dei casi di legittima riduzione del capitale sociale e sotto qualsiasi forma, restituisca ai soci i conferimenti o li liberi dall'obbligo di eseguirli.
- **Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.)** – Tale figura di reato ricorre nel caso in cui gli amministratori della Banca ripartiscano utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva, ovvero ripartiscano riserve, anche non costituite con utili, che non possono per legge essere distribuite.
- **Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.)** - Tale figura di reato si configura qualora gli amministratori della Banca acquistino o sottoscrivano, al di fuori dei casi previsti dalla legge, azioni o quote sociali, cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge.
- **Operazioni in pregiudizio dei creditori (art. 2629 c.c.)** – Tale figura di reato si realizza nel caso in cui gli amministratori della Banca violando le disposizioni di legge a tutela dei creditori, effettuino riduzioni del capitale sociale o fusioni con altra società o scissioni, cagionando danno ai creditori.
- **Omessa comunicazione del conflitto di interessi (Art. 2629 bis c.c.)** – L'amministratore, che in una determinata operazione ha, per conto proprio o di terzi, interesse in conflitto di interessi con quello della Società, non ne dà debita comunicazione agli altri amministratori e non si astiene dal partecipare alle deliberazioni riguardanti l'operazione stessa.

- **Formazione fittizia del capitale (art. 2632 c.c.)** – Tale figura di reato si configura qualora gli amministratori e i soci conferenti della Banca anche in parte, formino od aumentino fittiziamente il capitale sociale mediante attribuzioni di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale, sottoscrizione reciproca di azioni o di quote, sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione.
- **Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)** - Tale fattispecie di reato si configura nell'ipotesi in cui l'eventuale liquidatore di società, ripartendo i beni sociali prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie per soddisfarli, cagioni danno ai creditori stessi.
- **Corruzione tra privati (art. 2635 c.c.):** Tale fattispecie di reato si può configurare qualora un esponente della Banca dia o prometta denaro o altra utilità ad un esponente di una società (amministratore, direttore generale, dirigente preposti alla redazione dei documenti contabili societari, sindaco, liquidatore o soggetti sottoposti alla direzione e vigilanza dei primi), affinché questo compia od ometta atti (ad es. accordi un importante contratto alla Banca per un corrispettivo molto superiore alla media), in violazione degli obblighi inerenti al suo ufficio o degli obblighi di fedeltà, cagionando nocumento alla società.
- **Art. 2636 c.c. – Illecita influenza sull'assemblea** – Il reato si attua qualora con atti simulati o con frode si determini la maggioranza in assemblea allo scopo di procurare a sé o ad altri un ingiusto profitto. Tale reato può essere commesso da chiunque ("reato comune"), e quindi anche da soggetti esterni alla Società. La commissione di questo reato non si configura in quanto CSI è socio unico.
- **Aggiotaggio (art 2637 c.c.)** – Tale fattispecie di reato ricorre qualora, ad esempio, il soggetto apicale di società diffonda notizie false ovvero ponga in essere operazioni simulate o altri artifici idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati, ovvero ad incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o di gruppi bancari.
- **Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art 2638 c.c.)** – Tale fattispecie di reato si realizza qualora nelle comunicazioni alle autorità di vigilanza previste ai sensi della normativa applicabile in materia si esponano fatti materiali non corrispondenti al vero, ovvero si occultino con altri mezzi fraudolenti fatti che si sarebbero dovuti comunicare, al fine di ostacolare l'esercizio delle funzioni di vigilanza*.

*Relativamente al reato di "Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza", risultano a rischio tutte le aree funzionali di Credit Suisse Italy nello svolgimento della loro attività giornaliera.

La persona fisica che commette un reato societario è punita con la reclusione da un minimo sei mesi ad un massimo di otto anni e con una multa fino a 10.329 Euro.

Per la Società sono previste sanzioni pecuniarie da 100 a 1.000 quote (da 258 mila Euro a 1.549 mila Euro).

Con specifico riferimento al reato di corruzione tra privati, per la Società è prevista una sanzione pecuniaria da 200 a 400 quote (da 516 mila Euro a 1032 Euro).

9.2 Processi/Aree a rischio e Business Unit coinvolte

In considerazione della struttura e delle attività svolte la Banca, tramite l'attività di control and risk self assessment condotta (cfr. capitolo 4.2.1 "Approccio metodologico"), ha individuato i seguenti Processi/Aree a rischio con riferimento ai reati societari:

- contabilità e bilancio;
- segnalazioni e rapporti con le Autorità di Vigilanza;
- gestione delle informazioni price sensitive.

Nella tabella di sintesi sono indicate le Business Unit a cui fanno capo la gestione e il governo dei Processi/Aree a rischio sopra indicati:

		Direzione Executive Board Collegio Sindacale	Regional Management (BPPM e ORM)	PB: Canali distribuiti	Corporate Advisory	Advisory and Sales (AOF, Product and Services, Investment Consulting)	PB: FOS Casse	CP&D	AM: Canali distribuiti	AM: Portfolio Management and Product Control	Internal Audit	Direttore Compliance	Direttore Legal	Operations	Informations Technology	Credit Manager	CRES - Immobili Servizi/Sicurezza e Prevenzione	Direttore Ufficio Acquisti - Supply Mgmt	Direttore Risorse Umane	Direttore Financial Accounting
FATTI SOCIETARI	False comunicazioni societarie in danno di soci/creditori	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	SI
	Falso in prospetto	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
	Impedito controllo	SI	SI	NO	NO	NO	NO	NO	NO	NO	NO	SI	SI	NO	NO	NO	NO	NO	NO	SI
	Formazione fittizia del	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	SI
	Indebita restituzione dei conferimenti	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
	Illegale ripartizione degli utili e delle riserve	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	SI
	Illecite operazioni sulle azioni	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	SI
	Operazioni in pregiudizio dei creditori	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	SI
	Indebita ripartizione dei beni sociali da parte dei liquidatori	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	SI
	Illecita influenza sull'assemblea	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
	Aggiotaggio	SI	NO	NO	SI	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
	Ostacolo all'esercizio delle	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
Omessa comunicazione del conflitto d'interessi	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	

Con specifico riferimento al reato di corruzione tra privati (art. 2635 c.c.), introdotto tra i reati societari di cui all'art. 25-ter D.Lgs. 231/2001 dalla Legge 190/2015, nel corso delle attività di control and risk self assessment condotte nel corso del 2015 sono stati individuati i seguenti ambiti di attività potenzialmente a rischio 231 (identificati anche come Processi/Aree a rischio):

a. Processi/Aree a rischio diretti, ossia processi più specificatamente a rischio di commissione del reato di corruzione tra privati:

- *gestione delle attività di distribuzione e negoziazione con riferimento ai clienti "istituzionali": fondi pensione (occupazionali e pre-esistenti), casse di previdenza, compagnie di assicurazione, fondazioni bancarie;*
- *gestione delle attività di sviluppo commerciale per la distribuzione di prodotti Credit Suisse nei canali Retail e Wholesale;*
- *gestione delle attività di marketing per la Divisione Asset Management (selezione, negoziazione, formalizzazione, pagamento);*
- *attività di origination e negoziazione dei contratti con la clientela "Private Banking" per i servizi di consulenza e gestione (suddivisi in relazione alla segmentazione della tipologia clientela target: imprenditori, UHNWI...);*
- *gestione della vendita di prodotti strutturati alla Clientela Professional;*
- *gestione dei segnalatori (selezione, contrattualizzazione, pagamento);*
- *attività di origination e negoziazione dei servizi di corporate advisory;*
- *fatturazione dei servizi di corporate advisory;*
- *gestione degli agenti (selezione, contrattualizzazione, ecc.);*
- *gestione del sistema di remunerazione e incentivazione dei banker (dipendenti);*
- *gestione del sistema di remunerazione e incentivazione degli agenti;*
- *selezione del personale;*
- *gestione delle attività di marketing per la Divisione Private Banking (gestione ed organizzazione eventi, predisposizione di strumenti e materiale di comunicazione a supporto della funzione commerciale);*
- *attività di origination, negoziazione, erogazione e back-office relative alla sottoscrizione e gestione dei contratti relativi a prodotti creditizi (Lombard, anticipazioni fondiari, mutui, operazioni creditizie "Strutturate").*

b. Processi/Aree a rischio strumentali alla commissione del reato, tali dovendosi intendere quelle aree di attività caratterizzate dalla gestione di strumenti di tipo principalmente finanziario o nelle quali, pur non intrattenendosi rapporti diretti con società commerciali, si potrebbero creare le premesse per la commissione del reato.

I Processi Sensibili **strumentali** sono stati circoscritti ai seguenti

- *gestione acquisti e fornitori;*
- *gestione degli incarichi.*

Nella tabella di sintesi sono indicate le Business Unit a cui fanno capo la gestione e il governo dei Processi/Aree a rischio sopra indicati:

		Desk imprendi tori	Corporat e Advisory	PB COO	PB HEAD	Business Risk Manager	Marketin g strategic o	Products	Internal Audit	CRO Operatio nal Risk Manager	FOS / MIDDLE OFFICE	Distributi on	AM COO	Credit Risk Manage ment / Credit Consulta nt	TAX	Front Office	Business Process & Risk	HR	FINANCI AL ACCOUNT ING	EFFICIE NCY MANAGE MENT	LEGAL
CORRUZIONE TRA PRIVATI	Corruzione tra privati	SI	SI	SI	SI	NO	SI	NO	NO	NO	NO	SI	NO	SI	NO	NO	NO	SI	SI	SI	SI

9.3 Principi di controllo e di comportamento ed assetto del sistema di organizzazione, gestione e controllo

La presente sezione illustra le regole di condotta e di comportamento, nonché di assetto del sistema di organizzazione, gestione e controllo che dovranno essere seguite dai Destinatari al fine di prevenire il verificarsi dei Reati descritti al precedente Paragrafo 9.1

All'uopo, è fatto **divieto** in particolare di tenere i seguenti comportamenti/effettuare le seguenti operazioni:

- a) impedire od ostacolare in qualunque modo, anche occultando documenti o utilizzando altri idonei artifici, lo svolgimento delle attività istituzionali di controllo;
- b) determinare o influenzare illecitamente l'assunzione delle delibere assembleari, ponendo a tal fine in essere atti simulati o fraudolenti che si propongano di alterare artificiosamente il normale e corretto procedimento di formazione della volontà assembleare;
- c) rappresentare o trasmettere per l'elaborazione e la rappresentazione di bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della Banca;
- d) omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Banca;
- e) illustrare i dati e le informazioni utilizzati in modo tale da fornire una presentazione non corrispondente all'effettivo giudizio maturato sulla situazione patrimoniale, economica e finanziaria della Banca e sull'evoluzione della sua attività, nonché sugli eventuali strumenti finanziari e relativi diritti;
- f) compiere azioni o tenere comportamenti nei confronti di esponenti di società (siano esse Fornitori, Consulenti, ecc.) che siano o possano essere interpretati come pratiche di corruzione, favori illegittimi, comportamenti collusivi, sollecitazioni, dirette o mediante terzi, di privilegi per sé o per altri rilevanti ai fini della commissione del reato di corruzione tra privati;
- g) distribuire o ricevere omaggi commerciali, regali o altre utilità (inclusi pasti, viaggi e attività di intrattenimento) che possano costituire violazione di leggi o regolamenti o siano in contrasto con il Codice Etico o il Codice di Condotta, o possano - se resi pubblici - costituire un pregiudizio, anche solo di immagine, per la Banca. In particolare, non è consentito offrire denaro o utilità di qualsiasi tipo (promesse di assunzione, etc.) o compiere atti di cortesia commerciale, salvo che si tratti di utilità di modico valore ed elargite nel rispetto delle Procedure aziendali e del sistema di autorizzazioni ivi previsto, e sempre che comunque non possano essere in alcun modo interpretate quale strumento per influenzarli nell'espletamento dei loro doveri o per indurli a violare i loro obblighi d'ufficio o di fedeltà (sia affinché agiscano in un dato senso od omettano di agire), per ricevere favori illegittimi e/o per trarne indebito vantaggio. I regali offerti - salvo quelli di modico valore - devono essere documentati in modo adeguato per consentire le prescritte verifiche;
- h) allo stesso modo è vietato ai dipendenti e agli altri destinatari, così come ai loro familiari, accettare omaggi, regali o altri benefici che possano influenzare la loro indipendenza di giudizio o che possano compromettere la reputazione della Banca. A tal fine, ogni dipendente e destinatario deve evitare situazioni in cui interessi di natura personale possano essere in conflitto con quelli della Banca, attenersi alle procedure aziendali e ai sistemi di autorizzazione ivi previsti;
- i) riconoscere, in favore dei Fornitori, Consulenti, e/o collaboratori esterni, compensi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alla prassi vigente nel settore di attività interessato;

- ai Destinatari è fatto assoluto divieto di diffondere, concorrere a diffondere, in qualunque modo, informazioni, notizie o dati falsi o porre in essere operazioni fraudolente o comunque fuorvianti in modo anche solo potenzialmente idoneo a provocare un'alterazione del prezzo di strumenti finanziari.
- agli amministratori (ovvero ai soggetti di cui all'art. 2639 c.c.) è vietato restituire, anche simulatamente, i conferimenti ai soci o liberarli dall'obbligo di eseguirli, fatte salve ovviamente le ipotesi di legittima riduzione del capitale sociale.
- agli amministratori (ovvero ai soggetti di cui all'art. 2639 c.c.) è vietato ripartire utili o acconti su utili non effettivamente conseguiti, o destinati per legge a riserva, ovvero ripartire riserve, anche non costituite con utili, che non possono per legge essere distribuite.
- agli amministratori (ovvero ai soggetti di cui all'art. 2639 c.c.) è vietato effettuare riduzioni del capitale sociale o fusioni con altre società o scissioni in violazione delle norme di legge, con ciò cagionando un danno ai creditori.
- agli amministratori (ovvero ai soggetti di cui all'art. 2639 c.c.) è vietato formare o aumentare fittiziamente il capitale sociale mediante attribuzioni di azioni per somma inferiore al loro valore nominale, sottoscrizione reciproca di azioni o quote, sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti, ovvero del patrimonio sociale in caso di trasformazione.

Ai fini dell'attuazione dei divieti suddetti, dovranno rispettarsi le regole di seguito indicate:

- i Destinatari devono: a) comportarsi sempre con diligenza, correttezza e trasparenza, nell'interesse del pubblico degli investitori e del mercato; b) organizzarsi in modo da escludere la ricorrenza di situazioni di conflitto di interesse e, in tali occasioni, assicurare comunque l'equilibrata tutela degli interessi in conflitto; c) adottare misure affinché non si realizzi un'indebita circolazione/diffusione, all'interno di CSI, di informazioni rilevanti;
- i soggetti obbligati per legge a comunicare l'esistenza di un potenziale conflitto di interesse con la Banca sono tenuti a darne puntuale comunicazione nei tempi e nei modi prescritti dalla normativa vigente, astenendosi dal porre in essere atti pregiudizievoli per la società.
- mantenere un comportamento corretto, trasparente e collaborativo al fine di garantire la tutela del risparmio degli investitori;
- porre la massima attenzione ed accuratezza in ogni attività finalizzata all'acquisizione, elaborazione ed illustrazione di dati e di informazioni relative a prodotti finanziari necessari per permettere agli investitori di formare un fondato giudizio sulla situazione patrimoniale, economica e finanziaria della Banca e del Gruppo;
- i rapporti con il Collegio Sindacale e la Società di Revisione sono intrattenuti dal Responsabile dell'Unità Organizzativa di riferimento o dai soggetti dal medesimo appositamente incaricati;
- l'Organo Dirigente, i procuratori ed i dipendenti di CSI, devono attenersi scrupolosamente e rispettare eventuali limiti previsti nelle deleghe organizzative o procure conferite da CSI;
- tutti i dipendenti della Banca, i collaboratori (ivi compresi i lavoratori somministrati, i lavoratori a progetto) e i promotori finanziari (Personal Banker) sono tenuti a rispettare le Direttive e Procedure aziendali applicabili alle attività svolte nell'ambito delle Aree a Rischio;
- i Destinatari devono osservare una condotta improntata a principi di integrità, correttezza e trasparenza nell'attività di formazione del bilancio, delle relazioni e delle altre comunicazioni sociali previste dalla legge, in modo da fornire ai soci e al pubblico informazioni veritiere e corrette sulla situazione economica, patrimoniale e finanziaria di CSI, nel rispetto di tutte le norme di legge, regolamentari e dei principi contabili applicativi;
- deve essere garantita una tempestiva e completa evasione, a cura delle strutture competenti, delle 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 Unità Organizzativa 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;

- al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, l'Unità Organizzativa 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 delle attività relative alla gestione dei rapporti il Collegio Sindacale, i Comitati e la Società di Revisione;
- deve essere garantita una segregazione dei compiti tra i differenti soggetti coinvolti nel processo di gestione dei rapporti con il Collegio Sindacale, con i Comitati e la Società di Revisione;
- il processo di predisposizione dei documenti che contengono comunicazioni ai soci e/o al mercato relative alla situazione economica, patrimoniale e finanziaria della Banca prevede il coinvolgimento di distinte Unità Organizzative, operanti nelle diverse fasi del processo;
- le attività di predisposizione dei documenti che contengono comunicazioni ai soci e/o al mercato relative alla situazione economica, patrimoniale e finanziaria della Banca sono soggette a puntuali controlli di completezza e veridicità sia di sistema sia manuali, previa individuazione delle condizioni per l'eventuale comunicazione a terzi di informazioni riservate;
- i Destinatari devono garantire il puntuale rispetto di tutte le norme di legge che tutelano l'integrità e l'effettività del capitale sociale, al fine di non creare nocumeto alle garanzie dei creditori e, più in generale, ai terzi;
- ciascuna fase rilevante del processo di predisposizione dei Prospetti Informativi deve risultare da apposita documentazione scritta;
- al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, l'Unità Organizzativa di volta in volta interessata è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti per predisporre i Prospetti Informativi;
- eventuali situazioni di incertezza in ordine ai comportamenti da tenere (anche in ragione dell'eventuale condotta illecita o semplicemente scorretta del Pubblico Ufficiale), all'interpretazione della normativa vigente e delle Direttive e Procedure aziendali devono essere sottoposte all'attenzione del superiore gerarchico e/o all'OdV.

9.4 Procedure Specifiche

Ad integrazione delle regole di comportamento generali, devono rispettarsi le procedure specifiche di seguito descritte per le singole aree a rischio, nonché le ulteriori procedure di volta in volta adottate da CSI.

La Banca, inoltre, già precedentemente alla realizzazione della mappatura dei Processi/Aree a rischio aveva adottato, tra le altre, specifiche procedure e global policy per la disciplina dei Processi/Aree a rischio elencati al precedente paragrafo 9.2, provvedendo al loro costante e periodico aggiornamento.

Le principali procedure/global policy a disciplina dei Processi/Aree a rischio sono elencate nell'Allegato 1 (Matrice riepilogativa procedure).

Copia delle suddette procedure / policy globali è disponibile e consultabile nella Intranet aziendale.

9.4.1 Contabilità in bilancio

Il bilancio annuale deve essere redatto secondo i seguenti principi:

- rispetto di una procedura chiara e scandita per tempi, rivolta a tutte le funzioni coinvolte nelle attività di formazione del bilancio;
- redazione (esposizione e valutazione) dei documenti contabili ai fini civilistici italiani ai sensi dei Principi Contabili vigenti ed applicabili;
- correttezza nella redazione delle altre comunicazioni imposte o comunque previste dalla legge e dirette ai soci o al pubblico affinché le stesse contengano informazioni chiare, precise, veritiere e complete;
- verifica puntuale in ordine alla effettività e congruità delle prestazioni in relazione alle operazioni infragruppo che comportino acquisto o cessione di beni e servizi e, più in generale, corresponsione di compensi in relazione ad attività svolte nel contesto del gruppo: in particolare, le operazioni infragruppo e/o con società collegate devono sempre avvenire secondo criteri di correttezza sostanziale e devono essere previamente regolamentate sulla base di contratti stipulati in forma scritta, che devono essere trattenuti e conservati agli atti di ciascuna delle società contraenti. Dette condizioni devono essere regolate a condizioni di mercato, o equivalenti, sulla base di valutazioni di reciproca convenienza economica, avuto peraltro riguardo al comune obiettivo di creare valore per tutte le società del gruppo;
- tracciabilità delle operazioni che comportino il trasferimento e/o dilazione di posizioni creditorie, attraverso le figure della surrogazione, cessione del credito, l'accollo di debiti, il ricorso alla figura della delegazione, le transazioni e/o rinunce alle posizioni creditorie e delle relative ragioni giustificatrici;
- tracciabilità del processo relativo alle comunicazioni alle Autorità di Vigilanza da effettuare nel rispetto delle norme di legge e regolamenti, in vista degli obiettivi di trasparenza e corretta informazione. Agli eventuali incontri con le Autorità di Vigilanza (anche in sede ispettiva) devono intervenire i soggetti aziendali a ciò espressamente delegati; ogni incontro deve essere debitamente documentato. In caso di ispezione disposta dalle Autorità di Vigilanza, CSI assicura il coordinamento di tutte le funzioni aziendali interessate affinché sia garantita la più ampia e tempestiva collaborazione a dette Autorità, fornendo dati e documenti richiesti in modo tempestivo e completo;
- ogni singola Unità Organizzativa 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;
- il sistema dei poteri e delle deleghe stabilisce le facoltà di autonomia gestionale in relazione alle attività in oggetto, in particolare per quanto riguarda il passaggio a perdite;
- sono definiti diversi profili di utenza per l'accesso alle procedure informatiche ai quali corrispondono specifiche abilitazioni in ragione delle funzioni attribuite;
- la verifica dell'adeguatezza dei processi sensibili ai fini della informativa contabile e finanziaria nonché dei relativi controlli è affidata alla Funzione Financial Accounting
- i documenti che contengono comunicazioni ai soci e/o al mercato relative alla situazione economica, patrimoniale e finanziaria della Banca devono altresì essere redatti in base alle specifiche Direttive, Procedure, prassi e logiche aziendali in essere che:
 - identificano con chiarezza e completezza i soggetti interessati nonché i dati e le notizie che gli stessi 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;
 - prevedono la trasmissione di dati ed informazioni all'Unità Organizzativa responsabile della raccolta attraverso un sistema che consente la tracciabilità delle singole operazioni e l'identificazione dei soggetti che inseriscono i dati nel sistema;

9.4.2 Segnalazioni e rapporti con le Autorità di Vigilanza

- l'Organo Dirigente nonché i dipendenti di CSI devono: a) inviare alle Autorità di Vigilanza le segnalazioni previste dalla legge e dai regolamenti (incluse le Istruzioni di Vigilanza) o richieste ad altro titolo a CSI in modo tempestivo, completo ed accurato, trasmettendo a tal fine tutti i dati ed i documenti previsti o richiesti; b) indicare nelle predette segnalazioni dati rispondenti al vero, completi e corretti, dando indicazioni di ogni fatto rilevante relativo alla situazione economica, patrimoniale o finanziaria di CSI; c) evitare ogni comportamento che possa ostacolare le Autorità di Vigilanza nell'esercizio delle proprie prerogative (attraverso, ad esempio, mancanza di collaborazione, comportamenti ostruzionistici, risposte reticenti o incomplete, ritardi pretestuosi);
- i Destinatari devono improntare i rapporti con le Autorità di Vigilanza a criteri di integrità, correttezza, trasparenza e collaborazione, evitando comportamenti che possano in qualsiasi modo considerarsi di ostacolo alle attività che tali Autorità sono chiamate a svolgere. In tale prospettiva, i Destinatari devono evitare ogni comportamento che possa ostacolare le Autorità di vigilanza nell'esercizio delle proprie prerogative (attraverso, ad esempio, mancanza di collaborazione, comportamenti ostruzionistici, risposte reticenti o incomplete, ritardi pretestuosi).

Si confrontino inoltre le regole di comportamento specifiche indicate al paragrafo 8.4 e 8.5 Reati nei confronti della Pubblica Amministrazione.

9.4.3 Gestione delle informazioni price sensitive

- il trattamento delle informazioni deve essere condotto garantendo una adeguata riservatezza delle stesse. Tutte le informazioni a disposizione delle Società devono essere trattate nel rispetto della riservatezza e della privacy dei soggetti interessati secondo le procedure che la stessa ha assunto in ottemperanza alle vigenti normative in materia;
- nelle operazioni personali su strumenti finanziari poste in essere dai dipendenti e dai collaboratori (cfr direttiva GP00101 Transazioni in proprio dei collaboratori su titoli del Credit Suisse Group), dovranno essere rispettate rigorosamente tutte le procedure e le regole di cui si è dotata la Banca, sia che tali operazioni siano effettuate in nome e per conto proprio, sia per conto di terzi.

Si rimanda inoltre alle regole di comportamento descritte al paragrafo 11.4 Reati in materia di insider trading e market abuse.

9.4.4 Gestione delle attività di distribuzione e negoziazione con riferimento ai clienti "istituzionali", fondi pensione (occupazionali e pre-esistenti), casse di previdenza, compagnie di assicurazione, fondazioni bancarie

- sono chiaramente identificati i diversi soggetti coinvolti nelle varie fasi del processo. In particolare:
- la formulazione del pricing dei mandati di gestione istituzionale è effettuata a cura della funzione Distribution, che sottopone successivamente il pricing al Responsabile della Funzione Portfolio Management per una sua approvazione;
- i mandati di gestione e tutti i documenti predisposti per la partecipazione ai bandi di gara sono sempre sottoposti all'Ufficio Legal & Compliance Affairs per una sua approvazione e revisione;
- nel caso in cui un Cliente istituzionale venga acquisito con un processo "non standard", le diverse Funzioni coinvolte svolgono una verifica sulla fattibilità dell'acquisizione e redigono progetti *ad hoc* che coinvolgono i diversi uffici competenti (ad es. COO AM, BPMM, ecc.);
- la documentazione e le informazioni da ottenere in fase di acquisizione di un nuovo Cliente sono indicate all'interno di una check-list "Clienti Istituzionali", reperibile sul portale CSI;

- i rapporti intercorrenti tra CSI e il Cliente sono sempre formalizzati in appositi contratti scritti;
- gli accordi relativi alla distribuzione e commercializzazione dei servizi e dei prodotti sono sottoscritti con firma congiunta da parte di soggetti muniti dei necessari poteri, secondo un sistema di poteri formalizzato;
- la documentazione è conservata, ad opera della Funzione Distribution, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

9.4.5 Gestione delle attività di sviluppo commerciale per la distribuzione di prodotti Credit Suisse nei canale Retail e Wholesales

- le commissioni derivanti dall'attività promozionale e commerciale svolta da CSI nel Processo a rischio in esame sono definite nell'ambito di un Revenue Share Agreement regolarmente formalizzato tra CSI e C.S. (Luxembourg) SA;
- i rapporti relativi al Processo a rischio in esame sono formalizzati in contratti sottoscritti tra C.S. (Luxembourg) SA e il Cliente del canale Retail/Wholesale;
- la documentazione prodotta nell'ambito della gestione del rapporto con il Cliente dei canali Retail e Wholesales è conservata, ad opera della Funzione Distribution, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

9.4.6 Gestione delle attività di marketing per la Divisione Asset Management (selezione, negoziazione, formalizzazione, pagamento)

- CSI condivide annualmente con la Funzione Marketing di Credit Suisse AG il *budget* da destinare alle attività di marketing;
- tutte le iniziative di marketing devono essere preventivamente autorizzate via e-mail dal Responsabile della Funzione Marketing di Credit Suisse AG;
- per le iniziative di marketing di valore superiore a \$5000 deve essere compilato e sottoposto ad approvazione del Corporate Events il modulo online CERF;
- gli eventi di marketing vengono gestiti attraverso l'utilizzo di un apposito sistema informatico;
- i rapporti intercorrenti tra CSI e il fornitore che organizza l'evento di marketing vengono sempre formalizzati in appositi contratti;
- i fornitori e i consulenti coinvolti nel Processo a rischio in esame devono adottare un codice etico e impegnarsi a rispettare le prescrizioni previste dal Codice Etico e dal Modello 231 della Banca;
- il pagamento delle fatture presentate dai fornitori è autorizzato tramite l'utilizzo del tool SmartStream;
- la documentazione prodotta nell'ambito della gestione del rapporto con i fornitori esterni è conservata, ad opera della Funzione Distribution, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

9.4.7 Attività di origination e negoziazione dei contratti con la clientela "Private Banking" per i servizi di consulenza e gestione (suddivisi in relazione alla segmentazione della tipologia clientela target: imprenditori, UHNWI...)

- CSI ha previsto processi strutturati di classificazione del Cliente in funzione della tipologia (Retail o Professional) e del segmento di appartenenza (UHNWI, imprenditori, ecc.) dello stesso;

- la categoria di appartenenza del Cliente nonché il servizio prestato allo stesso (consulenza di base -ovvero Comfort-oppure avanzata, gestione) sono identificati nei sistemi gestionali di riferimento;
- nel caso in cui il Cliente sia rappresentato da una persona giuridica, l'Advisor verifica il titolare effettivo con il supporto della visura camerale depositata presso il Registro delle Imprese;
- CSI ha definito apposite check-list da compilare in fase di acquisizione del Cliente, strutturate sulla base delle direttive di Gruppo e della normativa in vigore in materia;
- il Line Manager/superiore gerarchico dell'Advisor verifica ed autorizza la check list di acquisizione del Cliente;
- la Funzione Operations esegue le verifiche sulla correttezza e completezza della documentazione richiesta e raccolta dagli advisor in fase di acquisizione del nuovo Cliente;
- il rendiconto inviato al Cliente riporta in modo distinto le commissioni applicate per i servizi di consulenza e quelle applicate per i servizi di gestione;
- il processo di acquisizione/onboarding del cliente è gestito con il supporto di sistemi gestionali;
- il modello di pricing (cd. "invest"):
 - è unico e standard;
 - è applicato sia in caso di Clienti rappresentati da persone fisiche che giuridiche;
 - è formalizzato nell'ambito di una matrice che definisce, in funzione dell'incrocio tra il patrimonio dato in gestione dal cliente e il grado di rischio dello stesso, dei range predeterminati di percentuale di commissione da applicare al cliente;
- i rapporti intercorrenti tra CSI e la Clientela Private Banking per i servizi di consulenza e gestione sono sempre formalizzati in appositi contratti scritti;
- il Processo a rischio in esame viene gestito secondo un sistema di poteri formalizzato. In particolare, i contratti con la clientela "Private Banking" vengono sempre sottoscritti con doppia firma da soggetti muniti dei necessari poteri;
- CSI ha elaborato un framework contrattuale standard ("modulo di apertura rapporti bancari consulenza e attivazione del servizio di consulenza e dei servizi esecutivi "CS Invest") che viene consegnato ai Clienti e che riporta i servizi di investimento offerti e le relative condizioni generali;
- dopo aver sottoscritto le condizioni generali dei servizi di investimento, per attivare i singoli servizi il Cliente deve sottoscrivere un conto amministrato CS Invest (per attivazione del servizio di consulenza) e/o un Private o Premium Mandate (per attivazione del servizio di gestione);
- le deroghe contrattuali applicabili sono chiaramente identificate in apposite tabelle ("Tabella Autorizzazioni") in cui sono specificati, per ogni deroga e per ogni Canale, l'Autorizzatore ed il limite espresso in percentuale entro il quale lo stesso può derogare, oltre che la scadenza della deroga stessa;
- le deroghe contrattuali non presenti nella "Tabella Autorizzazioni" sono sottoposte ad uno specifico iter autorizzativo;
- le deroghe sono gestite sia in modo automatico tramite l'utilizzo di un apposito sistema informatico, sia manualmente tramite moduli cartacei o mail il cui iter autorizzativo è chiaramente definito;
- sono eseguiti controlli sulle operazioni ritenute più a rischio sulla base di quanto definito nell'ambito di un Comitato, composto dal Responsabile del Private Banking (e da questi presieduto), dal Responsabile FOS/Middle Office e dal COO PRB CS Italy. Gli esiti di tali verifiche sono discussi nel corso degli incontri mensili del Comitato durante i quali vengono evidenziate le criticità maggiori e definite le attività da svolgere per limitare i rischi. Gli argomenti di discussione degli incontri vengono sempre formalizzati in appositi verbali;
- la documentazione prodotta in fase di acquisizione/onboarding del Cliente è conservata, a cura delle Funzioni coinvolte, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

9.4.8 Gestione della vendita di prodotti strutturati alla Clientela Professional

- CSI ha previsto processi strutturati di classificazione del Cliente in funzione della tipologia (Retail o Professional) e del segmento di appartenenza (UHNWI, imprenditori, ecc.) dello stesso;
- il cambio di categoria da Retail a Professional può essere effettuato solo su specifica richiesta del Cliente e deve sottostare a predeterminati criteri e condizioni;
- CSI ha redatto:
 - una c.d. “black list”, in cui sono riportati i prodotti/strumenti finanziari che non possono essere distribuiti e quindi acquistati da parte della clientela retail;
 - una c.d. “grey list”, in cui sono riportati prodotti/strumenti finanziari per i quali gli Advisor non possono offrire consulenza ma devono limitarsi a dare esecuzione alle operazioni disposte su iniziativa del Cliente, solo a seguito di una serie di verifiche e controlli secondo le procedure specifiche di riferimento;
- sono effettuati dei controlli specifici da parte delle Funzioni Business Risk Management e Compliance sulla corretta applicazione delle regole sancite dalle procedure in materia di distribuzione di prodotti complessi;
- i rapporti intercorrenti con i Clienti Professional in fase di distribuzione e collocamento dei prodotti finanziari strutturati vengono sempre formalizzati in appositi contratti scritti;
- il Processo a rischio in esame viene gestito secondo un sistema di poteri formalizzato. In particolare, i contratti con la Clientela Professional vengono sempre sottoscritti con doppia firma da soggetti muniti dei necessari poteri;
- la documentazione prodotta in fase di vendita di prodotti strutturati alla Clientela Professional è conservata, a cura delle Funzioni coinvolte, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

9.4.9 Gestione dei segnalatori (selezione, contrattualizzazione, pagamento)

- CSI ha chiaramente identificato i requisiti che il segnalatore deve possedere per essere considerato come tale dalla Banca;
- CSI richiede la compilazione, da parte del segnalatore e prima della sottoscrizione della lettera commissionale, di un modulo di *assessment*, che viene successivamente sottoposto all'approvazione da parte del Client Advisor e del Sector Head;
- la Funzione Commercial Reporting & Analysis e la Funzione Compliance svolgono verifiche in merito alla documentazione raccolta in fase di acquisizione del segnalatore;
- nei casi in cui il Cliente acquisito sia un soggetto indicato da un segnalatore autorizzato dalla Banca, l'Advisor deve sottoporre al Cliente, per sua sottoscrizione, la “Lettera di segnalazione cliente”;
- il compenso riconosciuto ai segnalatori è definito nell'ambito di una matrice predisposta da CSI;
- CSI predispone semestralmente un *file* di controllo, contenente l'elenco completo di tutti i Segnalatori e dei clienti dagli stessi introdotti, nonché le informazioni relative ai Clienti;
- la Funzione Compliance esegue controlli semestrali sul predetto file di controllo;
- con frequenza almeno biennale, il Client Advisor deve sottoporre la relazione con il Segnalatore ad una nuova procedura di valutazione;
- la fattura presentata dal segnalatore è soggetta ad autorizzazione e l'autorizzazione al pagamento viene rilasciata tramite l'utilizzo di un applicativo web;
- i rapporti intercorrenti con i segnalatori vengono sempre sottoposti al vaglio dell'AD per una sua approvazione formale e successivamente vengono formalizzati in “Lettere Commissionali”, che vengono sottoscritte dall'AD e vengono consegnate al Segnalatore corredate da un allegato 1 “Regole di comportamento” e un allegato 2 “Determinazione del compenso”;

- la documentazione prodotta nell'ambito del Processo a rischio in esame è conservata, a cura delle Funzioni coinvolte, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

9.4.10 Attività di origination e negoziazione dei servizi di corporate advisory

- la Banca ha predisposto una *checklist* di documenti che devono essere raccolti in fase di acquisizione del cliente;
- l'ufficio EMEA Conflict dept – Londra esegue un Conflict check al fine di verificare la presenza o meno di conflitti di interesse tra il Cliente e la Banca;
- tutte le transazioni vengono sottoposte, prima della sottoscrizione del mandato, all'autorizzazione del Local Mandate Approval Committee;
- la proposta/offerta nonché il mandato/engagement letter sono sottoposti a revisione da parte da parte dell'Ufficio Legal & Compliance Affairs;
- trimestralmente, tramite l'esecuzione dei cd. Controlli MICOS, viene svolta un'attività di monitoraggio dei *deal* conclusi;
- i rapporti intercorrenti con le società clienti vengono sempre formalizzati tramite il conferimento alla Banca di un mandato scritto;
- la documentazione prodotta nell'ambito del Processo a rischio in esame è conservata, a cura della Funzione Corporate Advisory, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

9.4.11 Fatturazione dei servizi di corporate advisory

- nell'*engagement letter*/mandato sottoscritto con il Cliente vengono sempre indicate le *success fees* e/o *retainer fees* riconosciute nonché le condizioni di pagamento;
- l'autorizzazione per la fatturazione dei servizi di Corporate Advisory ai Clienti è in capo alla funzione Corporate Advisory, che comunica alla funzione Financial Accounting quanto fatturare e le relative modalità;
- la documentazione prodotta nell'ambito del Processo a rischio in esame è conservata, a cura della Funzione Corporate Advisory e delle Funzioni coinvolte secondo competenza, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

9.4.12 Gestione degli agenti (selezione, contrattualizzazione, ecc)

- il processo di inserimento di un nuovo agente è formalizzato tramite la compilazione della Scheda Inserimento Advisor (SIA);
- la selezione degli agenti è soggetta alle attività di *background screening* svolte dalla funzione HR;
- il rapporto con gli agenti è sempre formalizzato nell'ambito di un contratto di agenzia, che stabilisce le condizioni generali nonché gli economics riconosciuti agli agenti;
- la documentazione prodotta nell'ambito del Processo a rischio in esame è conservata, a cura delle Funzioni coinvolte, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

9.4.13 Gestione del sistema di remunerazione e incentivazione dei banker (dipendenti)

Si confrontino le procedure specifiche previste per il Processo "Sistema degli incentivi" nella Parte 8 – Reati contro la Pubblica Amministrazione. Inoltre:

- CSI non effettua campagne di prodotto atte ad incentivare i banker alla vendita dei prodotti;
- il sistema di remunerazione dei banker non è legato alle vendite dei singoli prodotti, ma è definito sulla base delle *performance* del portafoglio e in generale dei risultati finali raggiunti;
- la gestione del sistema di valutazione delle performance dei banker è effettuata con il supporto di un apposito sistema informatico;
- gli obiettivi (composti da elementi qualitativi e quantitativi) dei singoli dipendenti sono precedentemente definiti dal dipendente in accordo con il superiore gerarchico;
- gli elementi quantitativi all'interno degli obiettivi e il grado di raggiungimento degli obiettivi stessi vengono decisi discrezionalmente dal superiore gerarchico del dipendente;
- le lettere con le quali vengono comunicati ai dipendenti gli incentivi e i premi vengono sottoscritte da soggetti muniti dei necessari poteri;
- la documentazione prodotta nell'ambito del Processo a rischio in esame è conservata, a cura delle Funzioni coinvolte, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

9.4.14 Gestione del sistema di remunerazione e incentivazione degli agenti

- gli schemi provvigionali sono definiti dal PB COO in accordo con la struttura commerciale, ovvero con il Responsabile Private Banking e il Responsabile Advisory & Sales;
- le provvigioni riconosciute degli agenti sono definite nell'ambito del contratto di agenzia sottoscritto tra le parti;
- le commissioni da riconoscere agli agenti sono calcolate con il supporto dei sistemi gestionali di riferimento a cura della funzione Commercial Planning & Development;
- le lettere con le quali vengono comunicati agli agenti gli incentivi e i premi vengono sottoscritte da soggetti muniti dei necessari poteri;
- la documentazione prodotta nell'ambito del Processo a rischio in esame è conservata, a cura delle Funzioni coinvolte, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

9.4.15 Selezione del personale

Si confrontino le procedure specifiche previste per il Processo "Gestione del personale" nella Parte 8 – Reati contro la Pubblica Amministrazione. Inoltre:

- ogni candidato è sottoposto ad un *background screening* circa la verifica e il riscontro delle informazioni dallo stesso fornite (precedenti penali, integrità finanziaria, precedenti occupazioni, titoli di studio e qualifiche professionali);
- eventuali eccezioni alle attività di *background screening* sono formalizzate in un modulo specifico e sottoposto a debita autorizzazione da parte di soggetti muniti dei necessari poteri;
- il processo di selezione del candidato deve prevedere perlomeno un colloquio tecnico a cura della Funzione Richiedente e un colloquio con la Funzione HR;
- una volta selezionato un candidato, la Funzione HR provvede a proporre l'ammontare del compenso al responsabile di *business* che ha richiesto l'assunzione, che deve approvarlo;
- l'*iter* di selezione (dal fabbisogno di risorsa alla sottoscrizione del contratto di assunzione) e il relativo processo autorizzativo vengono gestiti tramite il supporto di un sistema gestionale;
- i rapporti intercorrenti con i dipendenti vengono sempre formalizzati in appositi contratti di assunzione;
- nei contratti di assunzione è sempre inserita una clausola 231 di presa visione e impegno al rispetto del Codice Etico e del Modello Organizzativo adottati dalla Banca;

- la documentazione prodotta nell'ambito del Processo a rischio in esame è conservata, a cura della Funzione HR, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

9.4.16 gestione delle attività di marketing per la Divisione Private Banking (gestione ed organizzazione eventi, predisposizione di strumenti e materiale di comunicazione a supporto della funzione commerciale)

- l'evento di marketing è preceduto dalla stesura di una informativa, all'interno della quale si identificano il *target* ed il profilo dei clienti ai quali è rivolto l'evento;
- la candidatura per la partecipazione all'evento è sottoposta alla valutazione da parte dell'host dell'evento, solitamente rappresentato dal Sector Head;
- il lancio di un evento deve sottostare ad un *workflow* autorizzativo inserito in un apposito sistema informatico, determinato in funzione della tipologia e caratteristiche (importo) dello stesso;
- con cadenza mensile, la funzione Marketing Strategico redige un *report* relativo alle attività svolte e lo inoltra a una funzione di Shared Service in Polonia, che svolge un controllo di congruenza tra le registrazioni contabili e quanto presente nel sistema informatico utilizzato a presidio del Processo a rischio in esame;
- per gli eventi per i quali è prevista una spesa superiore ai 1.000 franchi per persona, è prevista la compilazione di un BAAC "Bank Anti-Corruption Compliance";
- il benessere al pagamento delle fatture presentate dai fornitori esterni è concesso dalla funzione Marketing Strategico;
- nell'ambito del contratto/ordine con i fornitori esterni, sono chiaramente indicati gli *economics* legati a capitoli specifici;
- i contratti con le agenzie di comunicazione e organizzazione eventi e i consulenti che assistono la Banca nello svolgimento delle attività di marketing sono sottoscritti da parte di soggetti muniti dei necessari poteri, secondo un sistema di poteri formalizzato;
- i fornitori e i consulenti coinvolti nel Processo a rischio in esame devono adottare un codice etico e impegnarsi a rispettare le prescrizioni previste dal Codice Etico e dal Modello 231 della Banca;
- la documentazione prodotta nell'ambito del Processo a rischio in esame è conservata, a cura della Funzione Marketing Strategico, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

9.4.17 Attività di origination, negoziazione, erogazione e back office relative alla sottoscrizione e gestione dei contratti relativi a prodotti creditizi (Lombard, anticipazioni fondiarie, mutui, operazioni creditizie "Strutturate")

- la formulazione dell'offerta al Cliente è predisposta a cura del Credit Consultant, in collaborazione sia con il Credit Risk Management che con il Legal & Corporate Affairs;
- CSI ha adottato metodologie di calcolo formalizzate per determinare il rischio creditizio;
- l'apertura della pratica di fido viene effettuata attraverso l'utilizzo di un apposito sistema informatico;
- il *pricing* delle richieste di apertura di credito è determinato dalla struttura commerciale, che autorizza eventuali deroghe sulla base di un *workflow* autorizzativo implementato nel sistema informatico utilizzato a presidio del Processo a Rischio in esame;
- la funzione Credit Risk Management svolge un'attività di monitoraggio continuo sulle posizioni creditizie;
- il contratto di apertura di credito sottoscritto con il cliente è sempre formalizzato e redatto secondo dei format standard predisposti con il supporto dell'ufficio Legal & Corporate Affairs;

- la documentazione prodotta nell'ambito del Processo a rischio in esame è conservata, a cura della Funzione Credit Risk Management, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

9.4.18 Gestione acquisti e fornitori

Si confrontino le procedure specifiche previste per il Processo "Gestione Acquisti e fornitori" nella Parte 8 – Reati contro la Pubblica Amministrazione.

4.4.20 Gestione degli incarichi

Si confrontino le procedure specifiche previste per il Processo "Gestione degli incarichi" nella Parte 8 – Reati contro la Pubblica Amministrazione.

9.5 Controlli dell'Organismo di Vigilanza

Con riferimento alle attività a rischio, l'Organismo di Vigilanza ha il compito di:

- verificare periodicamente il rispetto delle Procedure Amministrative e Contabili a supporto delle attività del Dirigente Preposto e l'esito dei controlli periodici;
- verificare periodicamente l'effettuazione delle comunicazioni alle Autorità di Vigilanza e l'osservanza delle procedure adottate nel corso di eventuali controlli;
- verificare che la società di revisione sia selezionata nel rispetto della procedura ed eventuali ulteriori incarichi di consulenza, aventi ad oggetto attività diversa dalla revisione contabile, non siano conferiti alla società di revisione, o alle società o entità professionali facenti parte dei medesimi network della società di revisione;
- controllare che le richieste inoltrate dagli organi di controllo siano tempestivamente recepite e evase;
- verificare che i rapporti con i Clienti siano in linea con i principi sanciti nel Codice di Condotta, nel Codice Etico e con le procedure aziendali;
- verificare la corretta applicazione delle procedure a disciplina dei Processi a rischio richiamati nella presente Parte Speciale.

10 REATI DI FALSITÀ IN MONETE, CARTE DI PUBBLICO CREDITO, IN VALORI DI BOLLO E IN STRUMENTI O SEGNI DI RICONOSCIMENTO**10.1 Fattispecie di reato**

L'Art. 25 bis del D.Lgs. 231/2001 comprende i seguenti reati previsti dal codice penale:

- Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate - (Art. 453 c.p.)
- Alterazione di monete – (Art. 454 c.p.)
- Spendita e introduzione nello Stato, senza concerto, di monete falsificate - (Art. 455 c.p.)
- Spendita di monete falsificate ricevute in buona fede - (Art. 457 c.p.)
- Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati - (Art. 459 c.p.)
- Uso di valori di bollo contraffatti o alterati - (Art. 464 c.p.)
- Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo - (Art. 460 c.p.)
- Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata - (Art. 461 c.p.)
- Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni - (Art. 473 c.p.)
- Introduzione nello Stato e commercio di prodotti con segni falsi - (Art. 474 c.p.)

Ogni possibilità di detenere, maneggiare o utilizzare denaro/valori di bollo può essere ritenuta sensibile per la realizzazione dei reati sopra elencati.

I maggiori rischi sono individuabili nelle ipotesi di messa in circolazione delle monete falsificate e di ricezione delle stesse al fine della messa in circolazione. In particolare, nella fattispecie di cui all'art. 457 (Spendita di monete falsificate ricevute in buona fede), potrebbe essere chiamato a rispondere del reato l'operatore che, anche solo dubitando della loro autenticità, utilizzi banconote contraffatte, ricevute in buona fede, al fine di evitare pregiudizio o inconvenienti alla banca nel rilevare e denunciare la falsità.

10.2 Processi/Aree a rischio

Nella tabella di sintesi sono indicate le aree individuate come sensibili alla commissione delle fattispecie di reato oggetto della presente sezione:

		Direzione Executive Board Collegio Sindacale	Regional Management (BPPM e ORM)	PB: Canali distribuiti	Corporate Advisory	Advisory and Sales (AOF, Product and Services, Investment Consulting)	PB: FOS Casse	CP&D	AM: Canali distribuiti	AM: Portfolio Management and Product Control	Internal Audit	Direttore Compliance	Direttore Legal	Operations	Information Technology	Credit Manager	CRES - Immobili Servizi/Sicurezza e Prevenzione	Direttore Ufficio Acquisti - Supply Mgmt	Direttore Risorse Umane	Direttore Financial Accounting
REATI FALSI VALORI	Falsità in monete (art.453, 454, 455, 457 c.p.)	NO	NO	NO	NO	NO	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
	Falsità in carte di pubblico credito (art. 460, 461 c.p.)	NO	NO	NO	NO	NO	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
	Falsità in valori di bollo (art. 459, 464 c.p.)	NO	NO	NO	NO	NO	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
	Contraffazione o alterazione marchi e brevetti (art. 473 c.p.)	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
	Introduzione e commercio prodotti con segni falsi (art. 474 c.p.)	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO

10.3 Principi di controllo e di comportamento ed assetto del sistema di organizzazione, gestione e controllo

Si fa espresso divieto di:

- accettare monete, banconote, valori di bollo senza i preventivi controlli, atti a rilevare l'autenticità del denaro e/o dei valori bollati;
- mettere in circolazione, in concorso o meno con terzi, valori falsi; si sottolinea che l'addetto che riceve in buona fede una banconota ed abbia, successivamente, dei dubbi sulla sua validità non deve tentare a sua volta di metterla nuovamente in circolazione ovvero restituire la banconota sospetta di falsità all'esibitore, tagliarla a metà o distruggerla;
- ☐ contravvenire a quanto previsto dalla normativa vigente in materia di ritiro dalla circolazione e trasmissione alla Banca d'Italia delle banconote denominate in euro sospette di falsità.

Anche per la prevenzione dei reati concernenti le falsità, devono essere rispettate le prescrizioni di seguito descritte:

- devono essere definiti idonei livelli autorizzativi nell'ambito di ciascuna fase operativa del processo. In particolare:
 - tutti i soggetti che intervengono nel processo di movimentazione di valori devono essere individuati e autorizzati (le responsabilità del Responsabile di filiale e dell'operatore di filiale sono descritte nel mansionario. Le filiali abilitate al maneggio di valori sono formalizzate tramite apposita circolare);
 - deve essere prevista la segregazione dei compiti tra i differenti soggetti coinvolti nel processo;
 - la stipula di rapporti contrattuali con intermediari addetti alla lavorazione dei valori deve essere autorizzata da soggetti a ciò facoltizzati in base al vigente sistema dei poteri e delle deleghe;
 - i soggetti che si trovano, nell'espletamento delle attività di propria competenza, a dover trattare valori devono essere appositamente incaricati e sono tenuti ad operare con onestà, integrità, correttezza e buona fede. Sono tenuti, inoltre, ad effettuare uno scrupoloso controllo sui valori ricevuti, al fine di individuare, ove presente, quelli sospetti di falsità. L'attività di identificazione può avvenire anche attraverso l'utilizzo di apparecchiature di selezione e accettazione delle banconote, atte a verificare sia l'autenticità sia l'idoneità alla circolazione delle banconote oppure a verificarne esclusivamente l'autenticità, oppure mediante controlli di autenticità da parte di personale addestrato, attraverso accertamenti manuali e senza l'ausilio di dispositivi di selezione e accettazione.
- in presenza di banconote sospette di falsità, gli addetti sono tenuti a predisporre tempestivamente un verbale di ritiro delle banconote sospette di falsità. Nello specifico, per quanto concerne le banconote in euro sospette di falsità, la normativa vigente prevede che l'addetto trasmetta una copia del verbale senza indugio e comunque entro il giorno lavorativo successivo alla verbalizzazione, all'Ufficio Centrale Antifrode dei Mezzi di Pagamento (UCAMP) del Ministero dell'Economia e delle Finanze a mezzo fax, e un'altra copia, unitamente alla banconota sospetta di falsità, alla Filiale della Banca d'Italia competente per territorio, entro il ventesimo giorno lavorativo successivo a quello in cui le banconote stesse sono state versate o depositate.
- le banconote sospette di falsità per le quali è stato redatto il verbale dovranno essere debitamente custodite da soggetti appositamente incaricati in idonei mezziforti nel periodo intercorrente tra la data di accertamento/ritiro del valore a quella di inoltro alla Banca d'Italia;
- il personale non può dare seguito e deve immediatamente segnalare per le azioni del caso al proprio Responsabile qualunque tentativo di messa in circolazione di banconote o valori

sospetti di falsità da parte della clientela o di terzi ove il personale risulti destinatario o semplicemente a conoscenza; il Responsabile a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta all'OdV;

- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione dei valori, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D.Lgs. 231/2001 e di impegno al suo rispetto;
- la corresponsione di onorari o compensi a fornitori di servizi eventualmente coinvolti è soggetta ad un preventivo visto rilasciato dall'unità organizzativa competente a valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi in favore di fornitori di servizi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto;
- l'esecuzione delle operazioni di messa in circolazione di valori deve prevedere l'utilizzo di sistemi informatici di supporto che garantiscano la tracciabilità delle operazioni effettuate;
- al fine di consentire la ricostruzione delle responsabilità, l'Unità Organizzativa di volta in volta interessata 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 di gestione dei valori, inclusa quella rimessa alla Banca d'Italia con riferimento alla trasmissione di banconote sospette di falsità.

11 REATI IN MATERIA DI INSIDER TRADING E MARKET ABUSE

11.1 Le fattispecie di reato

Tra i reati di Insider Trading (art.184 TUF) contemplati all'art. 25 sexies del Decreto 231, sono ricompresi i seguenti:

- **Manipolazione del mercato (artt. 185 e 187 ter del D.lg. 58/98 Testo Unico della Finanza).**

L'abuso di mercato realizzato attraverso l'alterazione delle dinamiche relative alla corretta formazione del prezzo di strumenti finanziari è punito dall'art. 185 TUF (manipolazione del mercato) sia da un illecito amministrativo, previsto dall'art. 187 ter TUF.

A differenza del caso dell'agiotaggio, ove vengono in considerazione strumenti finanziari non quotati o per i quali non sia stata presentata domanda di ammissione alla negoziazione in un mercato regolamentato, nel caso del reato e dell'illecito amministrativo di manipolazione del mercato, si tratta di strumenti finanziari quotati per i quali sia stata presentata richiesta di ammissione alla negoziazione su mercati regolamentati.

La condotta costitutiva del reato di manipolazione del mercato consiste:

- nella diffusione di notizie false (*information based manipulation*);
- nel compimento di operazioni simulate o di altri artifici idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari quotati o non quotati (*action based manipulation*).

L'illecito amministrativo di manipolazione del mercato (art. 187 ter) si configura invece nelle ipotesi di:

- diffusione, tramite mezzi di informazione, compreso INTERNET o ogni altro mezzo, di informazioni, voci o notizie false o fuorvianti che forniscano o siano suscettibili di fornire indicazioni false ovvero fuorvianti in merito agli strumenti finanziari;
- compimento di 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;
- compimento di operazioni od ordini di compravendita che consentano, tramite l'azione di una o più persone che agiscono di concerto, di fissare il prezzo di mercato di uno o più strumenti finanziari ad un livello anomalo o artificiale;
- realizzazione di altri artifici idonei a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di strumenti finanziari.

L'illecito amministrativo ha una sfera di applicazione molto più ampia rispetto al reato, dal quale si distingue in quanto è punibile anche a titolo di semplice colpa (e dunque per aver posto in essere le condotte sopra indicate per imprudenza, negligenza o imperizia) e non richiede l'idoneità delle informazioni, delle operazioni o degli artifici a provocare una sensibile alterazione del prezzo di strumenti finanziari.

- **Abuso di informazioni privilegiate (art. 184 e 187 bis del D.lg. 58/98 Testo Unico della Finanza).**

Le norme in esame puniscono l'abuso delle informazioni privilegiate conosciute in ragione dell'attività svolta attraverso il compimento di operazioni sugli strumenti finanziari cui le informazioni si riferiscono, ovvero attraverso la comunicazione – in forma diretta o indiretta – di dette informazioni.

Il reato e l'illecito amministrativo – meglio noti come *insider trading* – possono essere realizzati in vari modi:

- viene anzitutto in considerazione il c.d. trading, ossia l'acquisto, la vendita o il compimento di altre operazioni, direttamente o indirettamente, per conto proprio o per

conto di terzi, su strumenti finanziari, utilizzando informazioni privilegiate. E' opportuno al riguardo rimarcare che il divieto di utilizzazione comprende qualsiasi operazione su strumenti finanziari: non soltanto, dunque, l'acquisto o la vendita, ma anche riporti, permuta etc.;

- si parla invece di tipping a proposito della indebita comunicazione delle informazioni privilegiate ad altri. Più in particolare, l'ipotesi ricorre nel caso in cui l'insider primario comunichi la notizia privilegiata "al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio". Al riguardo, la comunicazione si ritiene lecita quando trova fondamento in norme che la consentano o la impongano ovvero nel contesto di prassi o usanze consolidate. Più in particolare, in riferimento ai gruppi societari, si ravvisa una comunicazione afferente il normale esercizio dell'ufficio nella trasmissione dei dati necessari alla formazione del bilancio consolidato (art. 43 D.Lgs. 127 del 1991 e art. 25, co. 4, D. Lgs. 356 del 1990), nonché nelle comunicazioni scambiate nel contesto dell'attività di direzione e coordinamento che oggi compete alla holding ai sensi dell'art. 2497 c.c., ovvero diffuse ai sensi dell'art. 114 TUF che impone, "fermi gli obblighi di pubblicità previsti da specifiche disposizioni di legge" agli emittenti quotati e ai soggetti che li controllano di comunicare al pubblico, senza indugio e secondo le modalità indicate dalla Consob, le informazioni privilegiate che riguardano direttamente detti emittenti e le società controllate;
- infine, viene in considerazione il c.d. tuyautage, ossia la raccomandazione o l'induzione di altri al compimento di una delle operazioni descritte in relazione ad informazioni privilegiate. In tale specifica ipotesi, l'insider non comunica a terzi l'informazione privilegiata, ma si limita – sulla base di questa – a consigliare o indurre terzi al compimento di una determinata operazione che egli sa, in virtù della notizia a sua conoscenza, idonea ad influire in modo sensibile sui prezzi di strumenti finanziari.

A chiunque, essendo in possesso di informazioni privilegiate a motivo della preparazione o esecuzione di attività delittuose, compie taluna delle azioni sopra elencate, si applica la relativa sanzione. La sanzione amministrativa si applica anche a chiunque, in possesso di informazioni privilegiate, conoscendo o potendo conoscere in base ad ordinaria diligenza il carattere privilegiato delle stesse, compie taluno dei fatti descritti.

Gli illeciti amministrativi (artt. 187 bis e 187 ter) prevedono fattispecie identiche a quelle contemplate come figure di reato dagli artt. 184 e 185: si tratta delle medesime condotte che danno luogo al tempo stesso ad un illecito penale e ad un illecito amministrativo quando siano commesse con il medesimo atteggiamento psicologico. Si ritiene che le sanzioni previste dalla due figure d'illecito si cumulino, dando luogo ad un concorso materiale di sanzioni.

La persona fisica che commette un reato finanziario è punita con la reclusione da un minimo di un anno ad un massimo di sei anni e con una multa fino a 5 milioni di Euro.

Per la Società sono previste sanzioni pecuniarie da 400 a 1.000 quote (da 1.032 mila Euro a 1.549 mila Euro).

Se, in seguito alla commissione dei reati, il prodotto o il profitto conseguito dall'ente è di rilevante entità, la sanzione è aumentata fino a dieci volte tale prodotto o profitto.

11.2 Nozione di "strumento finanziario" e "informazione privilegiata"

Per la commissione del suddetto reato dell'abuso di informazioni privilegiate è previsto necessariamente l'utilizzo di uno strumento finanziario per il quale si intendono: a) le azioni e gli altri titoli rappresentativi di capitale di rischio negoziabili sul mercato dei capitali; b) le obbligazioni, i titoli di Stato e gli altri titoli di debito negoziabili sul mercato dei capitali; b-bis) gli strumenti finanziari,

negoziabili sul mercato dei capitali, previsti dal codice civile; c) le quote di fondi comuni di investimento; d) i titoli normalmente negoziati sul mercato monetario; e) qualsiasi altro titolo normalmente negoziato che permetta di acquisire gli strumenti indicati nelle precedenti lettere e i relativi indici; f) i contratti «futures» su strumenti finanziari, su tassi di interesse, su valute, su merci e sui relativi indici, anche quando l'esecuzione avvenga attraverso il pagamento di differenziali in contanti; g) i contratti di scambio a pronti e a termine (swaps) su tassi di interesse, su valute, su merci nonché su indici azionari (equity swaps), anche quando l'esecuzione avvenga attraverso il pagamento di differenziali in contanti; h) i contratti a termine collegati a strumenti finanziari, a tassi di interesse, a valute, a merci e ai relativi indici, anche quando l'esecuzione avvenga attraverso il pagamento di differenziali in contanti; i) i contratti di opzione per acquistare o vendere gli strumenti indicati nelle precedenti lettere e i relativi indici, nonché i contratti di opzione su valute, su tassi d'interesse, su merci e sui relativi indici, anche quando l'esecuzione avvenga attraverso il pagamento di differenziali in contanti; j) le combinazioni di contratti o di titoli indicati nelle precedenti lettere.

Per informazione privilegiata si intende invece un'informazione di carattere preciso, che non è stata resa pubblica, concernente, direttamente o indirettamente, uno o più emittenti strumenti finanziari o uno o più strumenti finanziari, che, se resa pubblica, potrebbe influire in modo sensibile sui prezzi di tali strumenti finanziari. Un'informazione si ritiene di carattere preciso se: a) si riferisce ad un complesso di circostanze esistente o che si possa ragionevolmente prevedere che verrà ad esistenza o ad un evento verificatosi o che si possa ragionevolmente prevedere che si verificherà; b) è sufficientemente specifica da consentire di trarre conclusioni sul possibile effetto del complesso di circostanze o dell'evento di cui alla lettera a) sui prezzi degli strumenti finanziari.

Per informazione che, se resa pubblica, potrebbe influire in modo sensibile sui prezzi di strumenti finanziari si intende un'informazione che presumibilmente un investitore ragionevole utilizzerebbe come uno degli elementi su cui fondare le proprie decisioni di investimento.

Nel caso delle persone incaricate dell'esecuzione di ordini relativi a strumenti finanziari, per informazione privilegiata si intende anche l'informazione trasmessa da un cliente e concernente gli ordini del cliente in attesa di esecuzione, che ha un carattere preciso e che concerne, direttamente o indirettamente, uno o più emittenti di strumenti finanziari o uno o più strumenti finanziari, che, se resa pubblica, potrebbe influire in modo sensibile sui prezzi di tali strumenti finanziari.

11.3 Processi/Aree a rischio

Nella tabella di sintesi sono indicate le aree individuate come sensibili alla commissione delle fattispecie di reati di market abuse:

		Direzione Executive Board Collegio Sindacale	Regional Management (BPPM e ORM)	PB: Canali distribuiti	Corporate Advisory	Advisory and Sales (AOF, Product and Services, Investment Consulting)	PB: FOS Casse	CP&D	AM: Canali distribuiti	AM: Portfolio Management and Product Control	Internal Audit	Direttore Compliance	Direttore Legal	Operations	Information Technology	Credit Manager	CRES - Immobili Servizi/Sicurezza e Prevenzione	Direttore Ufficio Acquisti - Supply Mgmt	Direttore Risorse Umane	Direttore Financial Accounting
REATI FINANZIARI	Abuso di informazioni privilegiate	SI	SI	SI	SI	SI	NO	NO	SI	SI	NO	SI	SI	NO	NO	NO	NO	NO	NO	NO
	Manipolazione del mercato	SI	NO	SI	NO	SI	NO	NO	NO	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO

11.4 Principi di controllo e di comportamento ed assetto del sistema di organizzazione, gestione e controllo

La presente sezione illustra le regole di condotta e di comportamento, nonché di assetto del sistema di organizzazione, gestione e controllo che, dovranno essere seguite dai Destinatari al fine di prevenire il verificarsi dei Reati descritti al precedente Paragrafo 11.1.

All'uopo, è fatto **divieto** in particolare di tenere i seguenti comportamenti/effettuare le seguenti operazioni:

- compiere operazioni su strumenti finanziari di società appartenenti al Gruppo e/o di società terze in rapporto d'affari con la Banca o con il Gruppo stesso, in relazione alle quali si posseggano informazioni privilegiate circa l'emittente o il titolo stesso conoscendo o potendo conoscere in base ad ordinaria diligenza il carattere privilegiato delle stesse non rispettando le regole descritte nella policy "GP-00101 Transazioni in proprio dei collaboratori su titoli del Credit Suisse Group";
- compiere operazioni personali, per conto proprio o per conto terzi anche per interposta persona, utilizzando informazioni privilegiate acquisite in ragione delle proprie funzioni ed è vietato raccomandare o indurre altri a compiere operazioni utilizzando le predette informazioni privilegiate
- comunicare le medesime informazioni a terzi per ragioni diverse da quelle di ufficio (a titolo esemplificativo e non esaustivo: clienti, emittenti di titoli pubblicamente contrattati, ecc.) 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; particolare attenzione deve essere prestata nell'uso di telefoni cellulari e di telefoni "viva voce" onde evitate che le informazioni privilegiate possano essere ascoltate da estranei o comunque da soggetti che non hanno necessità di conoscerle;
- comunicare al mercato o ai media informazioni privilegiate relative alle società clienti della Banca, fatto salvo quanto previsto in materia di comunicazione al pubblico di informazioni privilegiate relative alla Banca. Qualora fosse richiesto un commento su specifiche operazioni relative a tali emittenti, ci si dovrà limitare a commentare i fatti già resi pubblici dall'emittente in base all'art. 114 del TUF; in ogni caso sono previsti obblighi di consultazione con le funzioni aziendali che sono legittimamente in possesso delle informazioni privilegiate;
- impedire il regolare svolgimento dell'attività aziendale nell'ambito della negoziazione di strumenti finanziari e gestione delle informazioni privilegiate, assicurando la corretta esecuzione dei controlli interni previsti dalla legge e dalle disposizioni di vigilanza;
- diffondere sia ad altro personale sia all'esterno della Banca, attraverso qualsiasi canale informativo, compreso internet, 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 Banca o al Gruppo e/o ai relativi strumenti finanziari nonché in relazione a società terze in rapporto d'affari con la Banca o il Gruppo e ai relativi strumenti finanziari;
- produrre e diffondere studi e ricerche in violazione delle norme, interne ed esterne, specificamente dettate per tale attività e, in particolare, senza comunicare nei modi richiesti dalla normativa gli interessi rilevanti e/o i conflitti eventualmente sussistenti;

Per completare il processo di implementazione delle sopra menzionate regole di condotta, devono essere rispettate le seguenti procedure, nonché le ulteriori procedure di volta in volta adottate dalla Succursale:

11 Procedure specifiche

La gestione e diffusione all'esterno delle informazioni rilevanti (che possono o potrebbero assumere anche la connotazione e natura di informazioni privilegiate), **delle comunicazione e la gestione delle relazioni esterne** deve avvenire nel rispetto delle seguenti prescrizioni specifiche:

- separatazza organizzativa (Chinese Walls) tra le Unità Organizzative che hanno a disposizione informazioni privilegiate e quelle che hanno rapporti diretti con il mercato, ivi compresi gli studi e ricerche aventi ad oggetto emittenti o strumenti finanziari quotati, le attività di trading (per conto proprio della Banca o di terzi, ivi comprese le gestioni di patrimoni) e le attività di sales;
- possono emettere comunicazioni in nome della Banca solo persone formalmente e preventivamente autorizzate o in via generale o per singole fattispecie;
- i rapporti con gli organi di informazione siano gestiti solo da soggetti autorizzati al fine di assicurare che le informazioni diffuse al pubblico siano veritiere e rispettino la regolamentazione vigente;
- tracciabilità del processo relativo alle comunicazioni alle Autorità di Vigilanza da effettuare nel rispetto delle norme di legge e regolamenti, in vista degli obiettivi di trasparenza e corretta informazione;
- tracciabilità del processo sia a livello di sistema informativo sia in termini documentali: in particolare, le operazioni di compravendita titoli sono gestite attraverso sistemi applicativi dedicati, nei quali sono mantenuti tutti i dettagli dei deal effettuati;
- obbligo di inoltro di tempestiva comunicazione all'Autorità di Vigilanza in caso di errori, omissioni o imprecisioni in materia di comunicazioni od operazioni aventi ad oggetto strumenti finanziari o comunque fatti idonei ad influire sul mercato;
- previa individuazione delle condizioni per l'eventuale comunicazione a terzi di informazioni riservate;
- rispetto di adeguate cautele volte a garantire la corretta gestione della documentazione contenente informazioni riservate in modo da impedire accessi indebiti;
- attività di controllo sulle operazioni di compravendita titoli eseguite sui mercati attraverso un sistema di controlli differenziato che tenga conto delle diverse tipologie di strumenti finanziari trattati e della specificità del mercato di riferimento;

Attività idonee a produrre un'influenza sul mercato

Tutti i soggetti che svolgono attività comunque connesse alla diffusione di notizie, anche a mezzo internet o qualsiasi altro mezzo di informazione, relative a strumenti finanziari e/o operazioni rilevanti ai fini della variazione del prezzo di detti strumenti, devono conformarsi a principi di trasparenza e correttezza, assicurando la tempestività, chiarezza, genuinità e completezza dei dati trattati e la parità di accesso alle informazioni.

E' pertanto fatto espressamente divieto di:

- compiere operazioni su strumenti finanziari di società appartenenti al Gruppo e/o di società terze in rapporto d'affari con la Banca o con il Gruppo, direttamente o indirettamente, per conto proprio o di terzi, non rispettando le regole descritte nella policy "GP-00101 Transazioni in proprio dei collaboratori su titoli del Credit Suisse Group"
- diffondere informazioni relative a strumenti finanziari o ad altre circostanze, che – in quanto imprecise, scorrette, false o comunque fuorvianti – possano astrattamente risultare idonee ad influire sul prezzo di strumenti finanziari.
- porre in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari;
- compiere operazioni o 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;
- compiere operazioni o ordini di compravendita che consentano, anche tramite l'azione di concerto di più persone, di fissare il prezzo di mercato di strumenti finanziari ad un livello anomalo o artificiale;
- compiere operazioni od ordini di compravendita che utilizzano artifici od ogni altro tipo di inganno o di espediente;

- utilizzare altri artifici idonei a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di strumenti finanziari;
- eseguire operazioni o impartire ordini di compravendita che rappresentano una quota significativa del volume giornaliero degli scambi dello strumento finanziario pertinente nel mercato regolamentato interessato, in particolare quando tali ordini o operazioni conducono ad una significativa variazione del prezzo dello strumento finanziario;
- eseguire operazioni o impartire ordini di compravendita avendo una significativa posizione in acquisto o in vendita su uno strumento finanziario che conducono a significative variazioni del prezzo dello strumento finanziario o dello strumento derivato collegato o dell'attività sottostante ammessi alla negoziazione in un mercato regolamentato;
- eseguire operazioni che non determinano alcuna variazione nella proprietà ovvero non comportano alcun trasferimento effettivo della proprietà di uno strumento finanziario ammesso alla negoziazione in un mercato regolamentato;
- eseguire operazioni o impartire ordini di compravendita che prevedono inversioni di posizione in acquisto o in vendita nel breve periodo e rappresentano una quota significativa del volume giornaliero di scambi dello strumento finanziario pertinente nel mercato regolamentato interessato e possono associarsi a significative variazioni del prezzo di uno strumento finanziario ammesso alla negoziazione in un mercato regolamentato;
- eseguire operazioni o impartire ordini di compravendita concentrati in un breve lasso di tempo nel corso della sessione di negoziazione e conducono a una variazione del prezzo che successivamente si inverte;
- impartire ordini di compravendita che modificano la rappresentazione dei migliori prezzi delle proposte di acquisto o di vendita di uno strumento finanziario ammesso alla negoziazione in un mercato regolamentato o, più in generale, la misura in cui essi modificano la rappresentazione del *book* di negoziazione a disposizione dei partecipanti al mercato, e sono revocati prima della loro esecuzione;
- seguire operazioni o impartire ordini nei momenti o intorno ai momenti utili per il calcolo dei prezzi delle aste di apertura o di chiusura, dei prezzi di controllo, dei prezzi di riferimento, dei prezzi di regolamento o di valutazione di strumenti finanziari, conducendo a variazioni di tali prezzi;
- eseguire operazioni o impartire ordini di compravendita facendo precedere o seguire dette operazioni dalla diffusione di informazioni false o fuorvianti da parte delle persone che hanno impartito gli ordini o eseguito le operazioni o da persone ad esse collegate;
- eseguire operazioni o impartire ordini di compravendita prima o dopo avere elaborato o diffuso, anche per il tramite di persone collegate, ricerche o raccomandazioni di investimento errate o tendenziose o manifestamente influenzate da interessi rilevanti.

In termini più specifici ed a titolo esemplificativo, si precisa inoltre che:

- in materia di *rumors*, ossia di diffusione di notizie non pubbliche in fase di chiusura o pre-apertura dei mercati, deve essere prevista l'informazione tempestiva, completa e corretta in relazione a notizie di dominio pubblico non comunicate al mercato e idonee a incidere sul prezzo di strumenti finanziari;
- quanto alle *informazioni previsionali*, aventi cioè ad oggetto dati relativi alla valutazione prospettica della situazione patrimoniale, economica e finanziaria del Gruppo o gli obiettivi quantitativi della sua gestione, deve essere garantita la correttezza, la continuità e la costanza delle informazioni, comunicando tempestivamente al mercato eventuali scostamenti significativi rispetto a quanto prospettato, ponendo particolare attenzione ai "risultati attesi dal mercato";
- con riferimento poi alle *informazioni confidenziali attinenti in particolare a progetti, trattative, manifestazioni di intenti*, la comunicazione al mercato sarà dovuta in tutte le ipotesi in cui trapelino notizie relative all'operazione imprecise o parziali, facendo espressa menzione dell'eventuale incertezza sull'esito finale della vicenda;
- con riferimento particolare agli eventuali *incontri con operatori di mercato*, si raccomanda il

rispetto delle regole che impongono la comunicazione preventiva alla Consob e alla società di gestione del mercato delle notizie rilevante in relazione ad esso (data, luogo, ora e principali argomenti), evitando nel contempo la comunicazione di informazioni previsionali di altre informazioni rilevanti, idonee a turbare il mercato.

- i rapporti con la stampa e con gli altri mezzi di comunicazione di massa sono riservati ad una specifica Funzione aziendale e devono svolgersi secondo specifiche Direttive e Procedure preventivamente fissate, nell'ambito delle quali assume particolare rilievo la previsione di punti di controllo sulla correttezza della notizia;
- i Destinatari nella diffusione di informazioni relative a strumenti finanziari, devono attenersi al rispetto dei principi di correttezza, trasparenza, completezza dell'informazione, tutela del mercato e rispetto delle dinamiche di libera determinazione del prezzo dei titoli;
- tutti i soggetti che svolgono attività comunque connesse alla diffusione di notizie, anche a mezzo internet o qualsiasi altro mezzo di informazione, relative a strumenti finanziari rilevanti ai fini della variazione del prezzo di detti strumenti, devono conformarsi a principi di trasparenza e correttezza, assicurando la tempestività, chiarezza, genuinità e completezza dei dati trattati e la parità di accesso alle informazioni.

Con riferimento alle operazioni su strumenti finanziari realizzate per conto o nell'interesse della Banca, è inoltre necessario che l'operazione:

- sia attuata con modalità e presenti caratteristiche tali da fornire al mercato indicazioni corrette, complete e tempestive;
- venga effettuata rispettando tutte le regole – normative e consuetudinarie – del mercato.
- sia posta in essere da soggetti individuati e legittimati al compimento delle operazioni stesse, nel rispetto della legge e delle normative interne;
- sia effettuata sulla base delle strategie previamente definite formalmente dai competenti organi e/o funzioni aziendali.

A complemento delle regole generali di condotta descritte in precedenza è inoltre presente un sistema di controllo a presidio dei processi riconducibili alla gestione di informazioni rilevanti/privilegiate e alla predisposizione e/o divulgazione di comunicati stampa e informativa al mercato. Tale sistema di controllo e di presidio si basa in particolare sui seguenti fattori:

- sono implementati i sistemi di sicurezza logica e fisica a garanzia della corretta gestione delle informazioni;
- è garantita la separazione funzionale (c.d. Chinese Walls) tra le funzioni organizzative appartenenti alle diverse Divisioni di Credit Suisse, progettata per gestire il flusso delle informazioni rilevanti/privilegiate (in particolare dai soggetti operanti nella c.d. "private side" ai soggetti operanti nel "public side") al fine di evitarne un'involontaria diffusione e/o un uso inadeguato;
- è garantita la separazione delle funzioni operative e di controllo, al fine di assicurare l'indipendenza dei controlli;
- è presente, a livello locale e globale/di Gruppo, un articolato sistema di Direttive, Procedure, meccanismi e strumenti, organizzativi, operativi ed informatici finalizzati a prevenire la commissione della fattispecie delittuose oggetto del presente paragrafo;
- è previsto il controllo automatizzato delle transazioni, con l'identificazione tempestiva delle operazioni potenzialmente sospette sulla base di parametri ed indici di anomalia predeterminati, che consente di evidenziare condotte vietate e i comportamenti che potrebbero integrarle;
- sono segnalate alla Consob le operazioni che, in base a ragionevoli motivi, possono essere ritenute sospette di condotte in violazione delle disposizioni normative.

11.6 Controlli dell'Organismo di Vigilanza

Con riferimento ai processi a rischio identificati, l'Organismo di Vigilanza ha il compito di:

- valutare l'efficacia e monitorare il rispetto dei principi definiti nel presente Modello, nel Codice di Condotta, nel Regolamento di Direzione, nella Policy GP-00101 Transazioni in proprio dei collaboratori sui titoli del Credit Suisse Group, in materia di trattamento delle Informazioni Privilegiate e Rilevanti per la prevenzione del reato di *market abuse*;
- verificare la corretta effettuazione delle comunicazioni alle Autorità di Vigilanza;
- verificare la corretta tenuta del Registro delle persone che hanno accesso alle Informazioni Privilegiate e Rilevanti;
- promuovere iniziative di formazione / informazione periodica relativamente ai reati ed agli illeciti amministrativi di abuso di mercato e delle relative regolamenti / procedure aziendali;

12 REATI TRANSNAZIONALI

I reati presupposto contenuti nella presente Parte Speciale sono disciplinati dall'art. 10 della L. 146/2006 "Ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea generale il 15 Novembre 2000 ed il 31 Maggio 2001".

12.1 Le Fattispecie di reato

Si considera reato transnazionale un reato che coinvolga un gruppo criminale organizzato e sia commesso in più di uno Stato:

- ovvero sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato;
- ovvero sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato;
- ovvero sia commesso in uno Stato ma abbia effetti sostanziali in un altro Stato.

L'art. 10 della L. 146/2006 annovera le fattispecie di reato di seguito indicate, quando assumono le caratteristiche di reato transnazionale:

Reati associativi:

- **Associazione per delinquere** – Associazione realizzata da tre o più persone allo scopo di commettere più delitti (**Art. 416 c.p.**)
- **Associazione di tipo mafioso** – Associazione di tipo mafioso formata da tre o più persone. L'associazione è di tipo mafioso quando coloro che ne fanno parte si avvalgono della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva per commettere delitti, per acquisire in modo diretto o indiretto la gestione o comunque il controllo di attività economiche, di concessioni, di autorizzazioni, di appalti e servizi pubblici o per realizzare profitti o vantaggi ingiusti per sé o per altri ovvero al fine di impedire od ostacolare il libero esercizio del voto o di procurare voti a sé o ad altri in occasioni di consultazioni elettorali (**Art. 416 bis c.p.**)
- **Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri** (Art. 291 quarter del Testo Unico di cui al DPR n. 43/1973)
- **Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope** (Art. 74 del Testo Unico di cui al DPR n. 309/1990)

Reati concernenti il traffico di immigrati:

- **Disposizioni contro le immigrazioni clandestine (Art. 12 D.Lgs. 286/1998)** – Reato commesso dal soggetto che, al fine di trarre profitto anche indiretto, compie atti diretti a procurare l'ingresso di taluno nel territorio dello Stato in violazione delle disposizioni del presente testo unico, ovvero a procurare l'ingresso illegale in altro Stato del quale la persona non è cittadina o non ha titolo di residenza permanente.

Reati di intralcio alla giustizia:

- **Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria** (Art. 377 bis c.p.) – Reato commesso dal soggetto che, con violenza o minaccia, o con offerta o promessa di denaro o di altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere davanti l'autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, quando questa ha la facoltà di non rispondere.
- **Favoreggiamento personale** – Reato commesso dal soggetto che, a seguito del verificarsi di un delitto per il quale la legge stabilisce la pena di morte o l'ergastolo o la reclusione, e fuori dei casi di concorso nel medesimo, aiuta taluno a eludere le investigazioni dell'Autorità, o a sottrarsi alle ricerche di questa (Art. 378 c.p.)

Per la Società sono previste sanzioni pecuniarie da 200 a 1000 quote (da 51,6 mila Euro a 1.549 mila Euro) e sanzioni interdittive (ad eccezione dei reati di intralcio alla giustizia, per i quali è prevista la sola sanzione pecuniaria) che vanno da tre mesi a due anni.

12.2 Processi/Aree a rischio

Nella tabella di sintesi sono indicate le aree individuate come sensibili alla commissione delle fattispecie di reati transnazionali:

		Direzione Executive Board Collegio Sindacale	Regional Management (BPPM e ORM)	PB: Canali distribuiti	Corporate Advisory	Advisory and Sales (AOF, Product and Services, Investment Consulting)	PB: FOS Casse	CP&D	AM: Canali distribuiti	AM: Portfolio Management and Product Control	Internal Audit	Direttore Compliance	Direttore Legal	Operations	Information Technology	Credit Manager	CRES - Immobili Servizi/Sicurezza e Prevenzione	Direttore Ufficio Acquisti - Supply Mgmt	Direttore Risorse Umane	Direttore Financial Accounting
REATI TRANSNAZIONALI	Associazione per delinquere	SI	NO	SI	SI	SI	NO	NO	SI	NO	NO	NO	NO	SI	NO	SI	NO	SI	SI	NO
	Associazione di tipo mafioso	SI	NO	SI	SI	SI	NO	NO	SI	NO	NO	NO	NO	SI	NO	SI	NO	SI	SI	NO
	Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	SI	NO
	Favoreggiamento personale	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	SI	NO
	Disposizioni contro le immigrazioni clandestine	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	SI	NO

12.3 Principi di controllo e di comportamento ed assetto del sistema di organizzazione, gestione e controllo

La presente Parte Speciale prevede l'espresso divieto a carico dei responsabili di funzione, dei dipendenti e dei collaboratori esterni di CSI di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle qui sopra esposte (art. 10 della Legge n. 146 del 16 Marzo 2006);
- sono altresì proibite le violazioni ai principi ed alle procedure aziendali previste nella presente Parte Speciale.

E' conseguentemente previsto 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 relative alla gestione del personale.

12.4 Procedure Specifiche

Le seguenti procedure specifiche per le singole aree a rischio integrano i principi generali di comportamento espressi nella Parte Generale del presente Modello, nonché le ulteriori procedure di volta in volta adottate dalla Banca.

12.4.1 Gestione fornitori e acquisti

Si confrontino le procedure specifiche previste per il processo "Gestione fornitori e acquisti" nella Parte 8 – Reati contro la Pubblica Amministrazione.

Nella selezione e valutazione di fornitori per contratti di importo significativo ovvero che presentino caratteristiche inusuali o anomale per tipologia o oggetto, le procedure devono inoltre prevedere:

- la valutazione e autorizzazione preventiva ai livelli autorizzativi più elevati;
- la comunicazione all'OdV della conclusione di tali contratti e le motivazioni a sostegno;
- la rivalutazione periodica del fornitore o immediata in caso sopravvenienza di profili di anomalia sia nei rapporti con il fornitore o nella tipologia delle richieste da questi avanzate;
- La comunicazione all'OdV di eventuali anomalie nelle prestazioni dovute dal fornitore, discordanze significative o ripetute tra materiale o servizio ricevuto rispetto a quanto concordato o particolari richieste avanzate dal fornitore alla banca.

12.4.2 Gestione del personale

Si confrontino le procedure specifiche previste per il processo "Gestione del personale" nella Parte 8 – Reati contro la Pubblica Amministrazione.

La Banca si dota di specifiche procedure che disciplinino i criteri generali di assunzione evitando ogni discriminazione o altra condotta illecita.

Si ribadisce l'assoluto divieto di assumere persone indicate nelle black list comunitarie o internazionali o facenti parte di organizzazioni presenti nelle stesse.

12.4.3 Gestione amministrativa clienti

Si confrontino le procedure specifiche previste per il processo "Gestione amministrativa clienti" nella Parte 13 Reati di terrorismo e nella Parte 17 Reati di riciclaggio

E' ribadito il divieto di porre in esecuzione operazioni in cui vi sia il sospetto della provenienza illecita di denaro, valori o altri beni da attività criminose o dalla partecipazione a tali attività (cc.dd. operazioni sospette).

12.4.1 Gestione del contenzioso giudiziale ed extragiudiziale

Si confrontino le procedure specifiche previste per il processo “Gestione del contenzioso giudiziale ed extragiudiziale” nella Parte 8 – Reati contro la Pubblica Amministrazione e nella Parte 19.3 Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

12.4.2 Erogazione del credito

Le procedure che regolano il **processo di erogazione del credito devono prevedere che:**

- sia verificata la professionalità ed il rispetto delle controparti, italiane ed estere, con cui la Banca si trova ad operare nello svolgimento della propria operatività;
- i comportamenti assunti dalle controparti commerciali non siano in contrasto con i valori etici fondamentali di Credit Suisse;
- tutti i dipendenti ed i collaboratori esterni agiscano nel rispetto del Codice di Condotta, del Regolamento di Direzione e delle procedure aziendali.

Si confrontino inoltre le procedure specifiche previste per il processo “Erogazione del credito” nella Parte Speciale 8 – Reati contro la Pubblica Amministrazione e nella Parte Speciale 18 Reati di Criminalità organizzata.

12.5 I controlli dell'Organismo di Vigilanza

L'Organismo di Vigilanza ha facoltà discrezionale di porre in essere controlli periodici sulle attività aziendali potenzialmente a rischio di commissione dei reati transnazionali, tra cui:

- verificare periodicamente il rispetto delle procedure interne in materia di selezione e valutazione dei fornitori non residenti;
-
- verificare la serietà ed il rispetto della legalità delle controparti con cui CSI si trova ad operare, attraverso il controllo dell'esistenza di pendenze penali in capo alla società estera o ai suoi amministratori;
- monitorare le attività di gestione del contenzioso (produzione e presentazione di atti e documenti, testimonianze, ecc.) e verificare che la Banca sia rappresentata in giudizio solo da soggetti che abbiano ricevuto una delega formale;
- verificare che non vi siano segnalazioni di comportamenti delle controparti commerciali che siano in contrasto con i valori etici fondamentali di CSI.

13 REATI CON FINALITÀ DI TERRORISMO

13.1 Le fattispecie di reato

Gli artt. 25 quater e 25 quater 1 del D.Lgs. 231/2001 **Delitti con finalità di terrorismo o di eversione dell'ordine democratico** comprendono i seguenti reati previsti dal codice penale:

- Associazione con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico **(Art. 270 bis c.p.)**
- Assistenza agli associati **(Art. 270 ter c.p.)**
- Arruolamento con finalità di terrorismo anche internazionale **(Art. 270 quater c.p.)**
- Addestramento con finalità di terrorismo anche internazionale **(Art. 270 quinquies c.p.)**
- Condotte con finalità di terrorismo **(Art. 270 sexies c.p.)**
- Attentato con finalità terroristiche o di eversione **(Art. 280 c.p.)**
- Atto di terrorismo con ordigni micidiali o esplosivi **(Art. 280 bis c.p.)**
- Sequestro di persona a scopo di terrorismo o di eversione **(Art. 289 bis c.p.)**
- Istigazione a commettere alcuno dei delitti previsti dai capi primo e secondo **(Art. 302 c.p.)**

Inoltre, l'art. 8 della Legge n. 7 del 9 gennaio 2006, riguardante le "Disposizioni concernenti la prevenzione e il divieto delle pratiche di mutilazione genitale femminile" ha introdotto all'interno della normativa sulla Responsabilità amministrativa il reato di pratiche di mutilazione degli organi genitali femminili previsto dal codice penale (art. 583 bis c.p.).

Si applicano sia sanzioni amministrative che interdittive.

Alla Società, nella cui struttura è commesso il delitto, si applica la sanzione pecuniaria da 200 a 700 quote se il delitto è punito con la reclusione inferiore a 10 anni, oppure da 400 a 1000 quote se punito con reclusione superiore a 10 anni.

13.2 Processi/Aree a rischio

Nella tabella di sintesi sono indicate le aree individuate come sensibili alla commissione delle fattispecie di reati con finalità di terrorismo:

		Direzione Executive Board Collegio Sindacale	Regional Management (BPPM e ORM)	PB: Canali distribuiti	Corporate Advisory	Advisory and Sales (AOF, Product and Services, Investment Consulting)	PB: FOS Casse	CP&D	AM: Canali distribuiti	AM: Portfolio Management and Product Control	Internal Audit	Direttore Compliance	Direttore Legal	Operations	Information Technology	Credit Manager	CRES - Immobili Servizi/Sicurezza e Prevenzione	Direttore Ufficio Acquisti - Supply Mgmt	Direttore Risorse Umane	Direttore Financial Accounting
REATI DI TERRORISMO	Reati con finalità di terrorismo o di eversione dell'ordine democratico (artt. 270-bis, 270-ter, 270 quater, 270 quinquies, 270 sexies, 280 c.p., 289-bis, 302)	SI	NO	SI	SI	SI	SI	NO	SI	NO	NO	NO	NO	NO	NO	NO	SI	NO	SI	NO

13.3 Principi di controllo e di comportamento ed assetto del sistema di organizzazione, gestione e controllo

La prevenzione dei reati aventi finalità di terrorismo o di eversione dell'ordine democratico si fonda sul rispetto, da parte della Banca, delle norme dettate per gli intermediari da Banca d'Italia (Unità di Informazione Finanziaria) in materia di antiriciclaggio e di segnalazioni di operazioni finanziarie sospette.

Il rischio che siano posti in essere i reati con finalità di terrorismo e di eversione dell'ordine democratico e i reati contro la persona riguarda principalmente, nell'ambito dell'attività bancaria, le attività di instaurazione dei rapporti con la clientela, di trasferimento di fondi, l'operatività di "sportello" ed, in particolare, il processo di erogazione del credito, attività che, ai fini della prevenzione dei reati in questione, si devono basare sul fondamentale principio dell'adeguata conoscenza della clientela. Tale principio rappresenta uno dei principali presupposti stabiliti dal D. Lgs. n. 231/2007 concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo.

In particolare la normativa in tema di finanziamento del terrorismo è incentrata sul decreto legislativo 22 giugno 2007 n. 109 che regola le modalità operative per eseguire le misure di congelamento di fondi e di risorse economiche stabilite:

- dalle Risoluzioni del Consiglio di sicurezza delle Nazioni Unite;
- dai regolamenti comunitari (c.d. "sanzioni finanziarie internazionali") per il contrasto del finanziamento del terrorismo e dei Paesi che minacciano la pace e la sicurezza internazionale.

Gli obblighi a carico della Banca consistono in:

- Misure del congelamento di fondi e di risorse economiche
- Obblighi di comunicazione all'Unità di Informazione Finanziaria le misure di congelamento
- Obblighi di segnalazione all'Unità di Informazione Finanziaria delle operazioni sospette di riciclaggio alle operazioni ed ai rapporti che, in base alle informazioni disponibili, possano essere riconducibili ad attività di finanziamento del terrorismo.

Per quanto precede, si individua quale attività sensibile in cui potrebbero presentarsi potenziali rischi per la commissione dei reati sopra illustrati l'attività aziendale sensibile inerente al contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminose.

Con riferimento ai reati in considerazione, è fatto divieto ai componenti degli organi sociali e ai dipendenti della Banca di effettuare operazioni con chiunque senza la preventiva fase d'istruttoria relativa all'identificazione ed alla valutazione dei nuovi clienti della Banca e delle attività da essi svolte.

Analoghe procedure di identificazione e valutazione devono essere adottate anche nelle fasi istruttorie relativamente ai processi di assunzione del personale e dei collaboratori e di acquisizione di nuovi fornitori.

A tal fine sono adottati idonei presidi volti ad assicurare la verifica puntuale delle apposite liste comunitarie ed internazionali contenenti i nominativi dei soggetti sottoposti a sanzioni finanziarie volte a contrastare e prevenire fenomeni di finanziamento del terrorismo.

Inoltre, sempre ai fini della prevenzione dei reati sopra citati, tutti i dipendenti dovranno attenersi alle Direttive e Procedure formalizzate per l'identificazione dei clienti e fornitori e per l'esecuzione di ordini di accredito o di pagamento, anche avvalendosi di elenchi/applicativi contenenti nominativi di soggetti coinvolti (o potenzialmente coinvolti) in attività terroristiche e dovranno registrare tutte le operazioni sospette come da Direttive e Procedure aziendali.

13.4 Procedure Specifiche

Si rimanda alle procedure specifiche previste per il processo di “Gestione del rischi in materia di contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminose” nella Parte Speciale 17 Reati di Riciclaggio.

13.5 Controlli dell’Organismo di Vigilanza

Si confrontino i controlli previsti all’analogia sezione nella Parte Speciale 17 Reati di Riciclaggio

14 DELITTI CONTRO LA PERSONALITA' INDIVIDUALE

14.1 Fattispecie di reato

Art.25- quinquies Delitti contro la personalità individuale

L'art. 5 della Legge n. 228 dell'11 agosto 2003, relativo alle misure contro il traffico di persone, introduce all'interno del Decreto Legislativo n. 231 il nuovo articolo 25-quinquies (articolo successivamente modificato dall'art. 10 della Legge n. 38 del 6 febbraio 2006), che comprende i seguenti reati previsti dal codice penale:

- Pratiche di mutilazione degli organi genitali femminili (**Art. 583 bis c.p.**)
- Riduzione o mantenimento in schiavitù o in servitù (**Art. 600 c.p.**)
- Prostituzione minorile (**Art. 600 bis c.p.**)
- Pornografia minorile (**Art. 600 ter c.p.**)
- Detenzione di materiale pornografico (**Art. 600 quater c.p.**)
- Pornografia virtuale (**Art. 600 quater.1 c.p.**)
- Iniziative turistiche volte allo sfruttamento della prostituzione minorile (**Art. 600 quinquies c.p.**)
- Tratta di persone (**Art. 601 c.p.**)
- Acquisto e alienazione di schiavi (**Art. 602 c.p.**)

Per la Società sono previste sanzioni pecuniarie da 200 a 1000 quote (da 51,6 mila Euro a 1.549 mila Euro) e le sanzioni interdittive previste dall'articolo 9 comma 2 per una durata non inferiore ad un anno.

14.2 Processi a Rischio

Relativamente ai reati previsti all'art. 25 quinquies del Decreto, non sono stati rilevati profili di rischio nel corso della fase di *assessment*.

14.3 Principi Generali di Comportamento

Relativamente ai reati previsti all'art. 25 *quinquies* del Decreto, non sono stati rilevati profili di rischio nel corso della fase di *assessment*.

14.4 Procedure Specifiche

Relativamente ai reati previsti all'art. 25 *quinquies* del Decreto, non sono stati rilevati profili di rischio nel corso della fase di *assessment*.

14.5 Controlli dell'Organismo di Vigilanza

Relativamente ai reati previsti all'art.25 *quinquies* del Decreto, non sono stati rilevati profili di rischio nel corso della fase di *assessment*, pertanto si lascia all'iniziativa dell'Odv la determinazione dei possibili controlli da svolgere a riguardo.

15 REATI IN TEMA DI SALUTE E SICUREZZA SUL LAVORO

15.1 Le fattispecie di reati in tema di salute e sicurezza sul lavoro

I reati presupposto contenuti nella presente sezione sono disciplinati dall'articolo 25 – septies del Decreto:

- **Omicidio colposo (art. 589 c.p.)**

L'art. 25 septies, primo comma, del Decreto introduce, quale reato sanzionato ai sensi del Decreto stesso, il delitto di omicidio colposo commesso con violazione dell'articolo 55, comma 26, del decreto legislativo attuativo della delega di cui alla legge 3 agosto 2007, n. 123, in materia di salute e sicurezza sul lavoro, ovvero del D.Lgs. n. 81/2008.

L'art. 25 septies, secondo comma, sanziona altresì il delitto di omicidio colposo di cui all'art. 589 del Codice Penale qualora esso sia commesso, in generale, con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

Ai sensi dell'art. 589 del Codice Penale, commette tale fattispecie di reato "chiunque cagiona per colpa la morte di una persona"; ai sensi del terzo comma del detto articolo, costituisce circostanza aggravante l'aver commesso il fatto con violazione delle "norme per la prevenzione degli infortuni sul lavoro".

Tale ipotesi di reato potrebbe configurarsi nel caso in cui la violazione colposa delle norme sulla tutela della sicurezza e salute sul lavoro, adottate in azienda, determini un incidente sul lavoro che cagioni la morte di un dipendente di CSI.

Ad esempio, in ipotesi di morte a seguito di un incendio divampato nei locali aziendali a causa di un cortocircuito del sistema informatico, in relazione al quale era stata negligenza omessa, da parte dei soggetti aziendali a ciò preposti, la periodica verifica di funzionalità e sicurezza.

- **Lesioni personali colpose gravi e gravissime (art. 590 c.p.)**

L'art. 25 septies introduce altresì, quale reato sanzionato dal Decreto, il delitto di lesioni personali colpose di cui all'articolo 590, terzo comma, del Codice Penale, commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

Ai sensi dell'art. 590 del Codice Penale, commette tale fattispecie di reato "chiunque cagiona ad altri, per colpa, una lesione personale"; costituisce circostanza aggravante, ai sensi del terzo comma del detto articolo, il fatto di aver cagionato la lesione personale con violazione delle "norme per la prevenzione degli infortuni sul lavoro".

Per lesioni gravi si intendono quelle consistenti in una malattia che metta in pericolo la vita o provochi una incapacità di attendere alle ordinarie occupazioni per un periodo superiore ai quaranta giorni, oppure in un indebolimento permanente di un senso o di un organo; per lesioni gravissime si intendono la malattia probabilmente insanabile, la perdita di un senso, di un arto,

⁶ Tale ultima disposizione stabilisce che, nei casi previsti dall'art. 55, comma 1, lett. a) del D.Lgs. n. 81/2008, ovvero nelle ipotesi in cui il datore di lavoro omette la valutazione dei rischi e l'adozione del documento di cui all'art. 17, comma 1, lett. a), ovvero lo adotta in assenza degli elementi di cui alle lettere a), b), d) ed f) dell'art. 28, e viola le disposizioni di cui all'art. 18, comma 1, lett. q) e z) prima parte, si applica la pena dell'arresto da sei mesi a un anno e sei mesi se la violazione è commessa:

a) nelle aziende di cui all'art. 31, comma 6, lett. a, b, c, d, f, ovvero:

- aziende industriali di cui all'art. 2 del D.Lgs. 334/99, soggette all'obbligo di notifica o rapporto;

- nelle centrali termoelettriche;

- negli impianti ed installazioni nucleari o che impiegano a qualsiasi titolo materiale radioattivo o che smaltiscono rifiuti radioattivi (D.Lgs. 230/1995, artt. 7, 28 e 33);

- nelle aziende per la fabbricazione e il deposito separato di esplosivi, polveri e munizioni;

- nelle industrie estrattive con oltre 50 lavoratori.

b) nelle aziende che svolgono attività che espongono i lavoratori a rischi biologici "gravi" (art. 268, I comma, lett. c e d), da atmosfere esplosive, cancerogeni mutanti e da attività di manutenzione, rimozione, smaltimento e bonifica di amianto;

c) per le attività disciplinate dal titolo IV ("cantieri temporanei o mobili") del D.Lgs. n. 81/2008 e caratterizzate dalla compresenza di più imprese e la cui entità presunta di lavoro non sia inferiore a 200 uomini-giorno.

di un organo o della capacità di procreare, la difficoltà permanente nella favella, la deformazione o lo sfregio permanente del viso.

Tale ipotesi di reato potrebbe configurarsi nel caso in cui la violazione colposa delle norme sulla tutela della sicurezza e salute sul lavoro determini un incidente sul lavoro che cagioni a un dipendente di CSI una lesione personale grave ovvero gravissima.

Ad esempio, qualora un dipendente di CSI subisca delle lesioni in seguito ad una caduta addebitabile alla presenza di arredo non a norma nei locali aziendali.

La persona fisica che commette il reato di omicidio colposo è punita con la reclusione da uno a dodici anni, diversamente la persona fisica che commette il reato di lesioni personali colpose gravi o gravissime è punita con la reclusione da due mesi a cinque anni.

Per la Società sono previste sanzioni pecuniarie (a partire da 10 mila Euro) e sanzioni interdittive non inferiori a tre mesi e fino ad un anno.

15.2 Processo di gestione dei rischi in materia di salute e sicurezza sul lavoro

Come anticipato nella Parte Generale al Capitolo 4 dedicato alla descrizione dell'approccio metodologico adottato per l'aggiornamento del Modello 231, con specifico riferimento alle analisi e valutazioni condotte in materia di sicurezza e salute sul luogo di lavoro, per sua natura tema pervasivo di ogni ambito ed attività aziendale, l'attenzione è stata posta su quello che può essere definito il sistema di **"gestione dei rischi in materia di salute e sicurezza sul luogo di lavoro"**.

I rischi in materia di sicurezza sono, per loro natura, insiti in ogni ambito ed attività aziendale; tuttavia, si è ritenuto opportuno identificare e mappare le aree/processi a maggiormente sensibili, in quanto specificatamente deputate dalla legge e dall'organizzazione interna a presiedere al processo di gestione di tali rischi.

Il Datore di lavoro è il principale garante della sicurezza all'interno dell'azienda (artt. 17 e 18 D.Lgs. 81/2008) e si avvale di altre figure aziendali (Dirigenti e Preposti) o esterne (RSPP) per l'attuazione ed il corretto funzionamento del sistema di gestione della salute e della sicurezza sul luogo di lavoro. Sono tuttavia da considerare come coinvolti nella gestione dei rischi in materia di salute e sicurezza sul lavoro tutti Dipendenti, collaboratori, Appaltatori, a prescindere dalla loro collocazione, dalla forma della loro collaborazione con la società, dalle loro mansioni svolte, dal loro livello gerarchico, in quanto sono obbligati a svolgere le loro attività nel rispetto del sistema delle regole e norme di riferimento, e ad adempiere agli obblighi e a rispettare le prescrizioni e divieti definiti nel suddetto sistema.

Il sistema di regole e norme in materia di salute e sicurezza sul lavoro è composto dai principi generali di condotta e comportamento e dai principi specifici definiti nei paragrafi 13.3 e 13.4 del presente Capitolo, sia dalla normativa vigente e dalle norme/linee guida a riguardo.

Le prescrizioni contenute

- nel Decreto Legislativo 9 aprile 2008, n. 81;
- nella norma BS OHSAS 18001:2007.

sono quindi da considerarsi complementari a quelle esplicitamente previste nel presente Modello.

Oltre agli aspetti trasversali del processo, come illustrato sopra, la gestione dei rischi in materia di salute e sicurezza sul lavoro prevede anche delle attività specifiche, demandate a figure aziendali individuate per ogni luogo di lavoro e a cui sia stato attribuito un ruolo specifico in materia di salute e sicurezza sul lavoro (con il supporto di altri soggetti aziendali o esterni, ove necessario/opportuno).

Questo processo può essere suddiviso nelle seguenti fasi e attività specifiche:

- Identificazione dei pericoli per la sicurezza e per la salute dei lavoratori;
- classificazione dei pericoli;

- Valutazione dei rischi [anche da interferenza];
- Individuazione delle misure di prevenzione e di protezione;
- Definizione di un piano di intervento di attuazione delle misure di prevenzione e di protezione;
- Realizzazione degli interventi pianificati;
- Attività di monitoraggio e controllo.

15.3 Processi a Rischio

Il rischio di potenziale commissione dei reati in oggetto è potenzialmente presente in tutte le attività operative svolte dai dipendenti o da collaboratori all'interno della sede di CSI.

Tuttavia, si ritiene opportuno individuare quali aree maggiormente sensibili al rischio, le funzioni specificatamente deputate al presidio della gestione del sistema di sicurezza in azienda.

Tali aree sono riportate nella tabella di sintesi qui di seguito:

		Direzione Executive Board Collegio Sindacale	Regional Management (BPPM e ORM)	PB: Canali distribuiti	Corporate Advisory	Advisory and Sales (AOF, Product and Services, Investment Consulting)	PB: FOS Casse	CP&D	AM: Canali distribuiti	AM: Portfolio Management and Product Control	Internal Audit	Direttore Compliance	Direttore Legal	Operations	Information Technology	Credit Manager	CRES - Immobili Servizi/Sicurezza e Prevenzione	Direttore Ufficio Acquisti - Supply Mgmt	Direttore Risorse Umane	Direttore Financial Accounting
REATI SICUREZZA SUL LAVORO	Omicidio colposo commesso con la violazione delle disposizioni di cui	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	SI	NO	NO	NO
	Omicidio colposo commesso con la violazione delle norme sulla tutela della	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	SI	NO	NO	NO
	Lesioni personali colpose gravi o gravissime commesse con la violazione	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	SI	NO	NO	NO

15.4 Principi generali di condotta e comportamento e di assetto del sistema di organizzazione, gestione e controllo

La presente sezione illustra le regole di condotta generali e di comportamento, nonché di assetto del sistema di organizzazione, gestione e controllo che, unitamente ai principi specifici sanciti nel paragrafo 15.5 dovranno essere seguite dai Destinatari al fine di prevenire il verificarsi dei Reati descritti nel Paragrafo 15.1.

Tutti dipendenti e collaboratori di CSI, inclusi gli Appaltatori nei rispettivi ambiti e per la propria competenza – sono tenuti a:

- rispettare le norme, gli obblighi e i principi posti dalla normativa vigente e dalle norme/linee guida in materia di salute e sicurezza contenute nel Decreto Legislativo 9 aprile 2008, n. 81 e nella norma BS OHSAS 18001:2007;
- rispettare i principi generali di condotta e comportamento, i principi di controllo e i principi specifici formulati nel presente Modello 231;
- promuovere il rispetto delle suddette norme, regole e principi ed assicurare gli adempimenti in materia di salute e sicurezza sul lavoro;
- adottare una condotta di massima collaborazione e trasparenza e rispettare i principi di condotta e comportamento specificati nel Capitolo 8 nei rapporti con gli enti pubblici competenti in materia salute e sicurezza sul lavoro, sia in fase di stesura e comunicazione di eventuali dichiarazioni, sia in occasione di accertamenti/verifiche ispettive;
- promuovere l'informazione e formazione interna in tema di rischi specifici connessi allo svolgimento delle proprie mansioni e attività, di struttura e regolamento aziendale in materia di salute e sicurezza, procedure e misure di prevenzione e protezione e/o prendere atto dell'informazione fornita e/o partecipare attivamente ai corsi di formazione;
- utilizzare correttamente i macchinari, le apparecchiature, gli impianti, i mezzi di trasporto e le altre attrezzature di lavoro, nonché i dispositivi di sicurezza;
- Segnalare ai Responsabili o ai soggetti responsabili per la gestione della salute e sicurezza e/o all'OdV (attraverso l'invio di una Segnalazione da effettuarsi nelle circostanze e secondo le modalità definite nell'ambito del Capitolo 6.6 della Parte Generale) violazioni delle norme definite, inefficacia dei mezzi di prevenzione e protezione ed ogni situazione di pericolo potenziale o reale.

15.5 Principi specifici e componenti del sistema di organizzazione, gestione e controllo

Esistenza e diffusione di disposizioni organizzative e di un sistema formalizzato di ruoli, poteri e deleghe con riferimento a salute e sicurezza sul lavoro, in particolare riferimento a:

- Individuazione del Datore di Lavoro all'interno del Consiglio di Amministrazione ed, eventualmente, del Delegato del Datore di Lavoro, in conformità con le disposizioni previste dalla normativa, formalizzazione della nomina in un documento e comunicazione del nominativo;
- Individuazione dei Dirigenti e Preposti della sicurezza in conformità con le disposizioni previste dalla normativa, formalizzazione della nomina in un documento e comunicazione del nominativo;
- Designazione del Responsabile del Servizio di Prevenzione e Protezione in conformità con le disposizioni previste dalla normativa, verifica dei requisiti formativi e professionali e formalizzazione della nomina;
- Nomina del Medico competente, in conformità con le disposizioni a riguardo previste dalla normativa, verifica dei requisiti formativi e professionali e formalizzazione della nomina;
- Elezione o designazione dei Rappresentanti dei lavoratori per la sicurezza in conformità con le disposizioni a riguardo previste dalla normativa, formalizzazione della individuazione in un documento e comunicazione del nominativo ai lavoratori;
- Formale costituzione del Servizio di Prevenzione e Protezione aziendale;

- Verifica periodica della legittimità, dell'adeguatezza e dell'efficacia del sistema di poteri e deleghe in materia di sicurezza e salute sul luogo di lavoro;
- Esistenza di un organigramma in materia di sicurezza che illustra graficamente i soggetti delegati alla tutela dei lavoratori, i ruoli e compiti di ognuno, indicando in specifico:
 - il Datore di lavoro;
 - il Delegato del Datore di lavoro e i dirigenti;
 - il Responsabile del Servizio di Prevenzione;
 - il Medico competente;
 - il Rappresentante dei lavoratori;
 - gli addetti alla prevenzione incendi e primo soccorso.

L'individuazione delle figure coinvolte nella gestione della salute e della sicurezza sul lavoro deve avvenire in forma scritta, con data certa, deve essere pubblicizzata all'interno dell'organizzazione e prevede l'accettazione formale dell'interessato.

Esistenza di policy, procedure e disposizioni operative formalizzate che disciplinano le attività dei soggetti coinvolti nel processo di salute e sicurezza sul lavoro, in particolare:

- Esistenza del documento "Politica della Sicurezza" che stabilisce chiaramente gli obiettivi generali riguardanti la salute e la sicurezza sul lavoro e un impegno al miglioramento delle prestazioni relative alla salute e alla sicurezza nel suo complesso e che è l'elemento di riferimento di tutto il processo. Il "datore di lavoro" ha altresì la responsabilità di diffondere il documento a tutti i soggetti direttamente e indirettamente interessati.
Nell'ipotesi di svolgimento di attività di lavoro in esecuzione di un contratto di appalto [e subappalto], d'opera o somministrazione, la politica della sicurezza è comunicata dal committente all'appaltatore, tramite l'inserimento nel documento unico di valutazione dei rischi da interferenza.
- Esistenza di un processo di pianificazione strategica che comprenda l'allocazione di risorse da destinare all'implementazione del modello di gestione della salute e della sicurezza sul lavoro, finalizzata a garantire l'efficacia delle misure cautelari e degli impianti, il costante adeguamento al progresso tecnologico, nonché un'opportuna attività di formazione;
- Esistenza e adeguata diffusione di una procedura che descrive le modalità per l'identificazione dei pericoli, per la valutazione dei rischi e per l'implementazione delle necessarie misure di controllo e che definisce i soggetti in capo ai quali sussiste tale obbligo. La procedura descrive i passi necessari per poter predisporre il conseguente Documento di Valutazione dei Rischi (vedi prossimo punto);
- Esistenza del Documento di Valutazione dei Rischi, in conformità a quanto disposto dagli articoli 28 e 29 del D.Lgs 81/08;
- Esistenza del Documento Unico di valutazione dei rischi da interferenze di cui all'articolo 26, comma 3 del D.Lgs. 81/08;
- Esistenza di procedure per la gestione, l'analisi dei cambiamenti ed il tempestivo aggiornamento del modello di gestione della sicurezza sul lavoro al verificarsi di modifiche sostanziali nell'organizzazione del lavoro, di gravi infortuni o di specifiche risultanze nell'attività di sorveglianza sanitaria oppure in funzione di significative evoluzioni della tecnica,
- Esistenza e adeguata diffusione di un Piano di Emergenza Interno, in conformità con i requisiti specificati nel D.Lgs 81/08 e dalle altre norme vigenti a disciplina dello specifico argomento;
- Esistenza di altre procedure, ordini di lavoro, ordini di servizio ed istruzioni operative che disciplinano per l'unità organizzativa di riferimento le modalità operative delle attività, delle verifiche, delle analisi, delle misure di protezione e prevenzione da svolgere in tema di salute e sicurezza.
- Esistenza di un programma di informazione, formazione ed addestramento periodico e sistematico dei dipendenti/collaboratori coinvolti nel processo della gestione dei rischi in materia di salute e sicurezza sul lavoro, in conformità con quanto previsto dal D.Lgs 81/08

e tracciabilità dell'avvenuta informazione e formazione dei lavoratori, documentando in particolare:

- data di formazione;
 - numero di ore dedicate alla formazione;
 - nominativo del docente;
 - qualifica del docente;
 - destinatari del corso;
 - programma;
 - strumenti di formazione;
 - obiettivi che il corso si pone;
 - criteri di verifica;
 - nominativo dei presenti e firma di presenza;
 - giudizio sull'apprendimento.
- Esistenza di un sistema disciplinare volto alla repressione, attraverso sanzioni proporzionate alla gravità del fatto, di trasgressioni alle disposizioni antinfortunistiche;

Attività di monitoraggio, di sorveglianza e di controllo operativo

1. Sistema di rilevazione degli infortuni, incidenti e non conformità:

Esistenza di una procedura, nella quale sono definiti e sostanzianti i termini infortunio, incidente, quasi infortunio, quasi incidente e non conformità e nella quale sono specificate:

- le metodologie e responsabilità di analisi ed indagine;
- le iniziative prese per la riduzione delle conseguenze scaturite;
- il controllo per la conferma dell'efficacia delle azioni preventive e correttive svolte;
- tenuta di un apposito registro degli infortuni, incidenti, quasi infortuni, quasi incidenti e non conformità;
- comunicazione degli infortuni all'INAIL, in conformità con art. 18 del D.Lgs. 81/2008 e nel rispetto dei principi di condotta sanciti nel capitolo dedicato ai rapporti con la Pubblica Amministrazione (Capitolo 8).

2. Sorveglianza sanitaria effettuata dal Medico competente, nei casi previsti dalla normativa vigente e in coerenza alle risultanze della valutazione dei rischi; formalizzazione del programma della sorveglianza in forma di Protocollo sanitario, verbalizzazione dei sopralluoghi effettuati, gestione della documentazione sanitaria, Relazione annuale dei dati sanitari aggregati.

3. Esecuzione di verifiche/audit periodici che sono programmati in base alla valutazione dei rischi. L'obiettivo di tale verifica è di esaminare se gli adempimenti, le norme e le prescrizioni specifiche come previsti dalla normativa vigente e dal presente Modello sono stati attuati e rispettati e se le misure di prevenzione e di protezione definite nel piano di intervento sono stati implementati. Questa attività di controllo può essere suddivisa nelle seguenti fasi:

- Redazione di un piano di audit annuale di verifica a cura dell'RSPP ed emanato dal Datore di Lavoro;
- Redazione/aggiornamento delle procedure operative che specificano l'ambito dell'audit, le modalità operative dell'audit e i soggetti che effettuano l'audit (interni o esterni) e le modalità di rendicontazione e comunicazione dei risultati;
- Effettuazione di analisi documentali (ad es. analisi di registri, controllo della presenza di certificati e certificazioni, valutazione dell'adeguatezza delle procedure, istruzioni, piani d'emergenza etc. esistenti in materia di salute e sicurezza), di sopralluoghi (ad es. controllo dei dispositivi di sicurezza o della segnaletica di sicurezza) o di analisi specifiche tecniche (ad es. analisi ambientali);

- Redazione di adeguata documentazione che rapporta i dettagli delle verifiche svolte e i risultati dell'audit. L'audit report è comunicato alle seguenti figure:
 - Datore di lavoro;
 - Responsabile del Servizio di Prevenzione e Protezione (se diverso dall'auditor);
 - Medico competente;
 - Rappresentante dei lavoratori per la sicurezza;
 - OdV.
- Verifica di scostamenti rilevanti rispetto al budget relativo ai costi della sicurezza e le motivazioni sottostanti

Tracciabilità e verificabilità ex post dei flussi informativi riferiti al Processo:

- ciascuna fase rilevante della gestione dei rischi in materia di salute e sicurezza sul lavoro deve risultare da apposita documentazione scritta;
- i flussi informativi tra i soggetti delegati alla tutela dei lavoratori e altri soggetti, con riguardo alle attività svolte nell'ambito del Processo in esame, sono adeguatamente salvate e archiviate in modo da garantire l'evidenza e la tracciabilità;
- le riunioni in materia di salute e sicurezza sono adeguatamente verbalizzate;
- predisposizione ed approvazione di una procedura diretta alla gestione e controllo dei dati e dei documenti che assicuri:
 - a) l'individuazione dei documenti di salute e sicurezza;
 - b) la definizione delle modalità di tenuta e archiviazione della documentazione;
 - c) l'individuazione del responsabile/dei responsabili per la gestione e l'archiviazione della documentazione;
 - d) il periodico riesame, la modifica o integrazione;
 - e) la disponibilità presso il luogo di lavoro e la diffusione a tutti gli interessati;
 - f) la sostituzione di tutti i documenti e le informazioni superate od obsolete;
 - g) l'archiviazione e conservazione ai fini legali e/o scientifici.

Altri controlli in materia di salute e sicurezza sul lavoro:

- Svolgimento di una riunione annuale del Servizio di Prevenzione e Protezione, in conformità con quanto previsto dal D.Lgs. 81/08 e verbalizzazione della riunione
- Consultazione e comunicazione a favore del Rappresentante dei lavoratori, in conformità con quanto previsto dal D.Lgs. 81/08, e formalizzazione del coinvolgimento dei lavoratori in una disposizione, nel quale sono elencati gli ambiti di consultazione obbligatorie e in cui sono definite le modalità e le responsabilità per le comunicazioni ai lavoratori;
- tenuta del registro di controllo delle attrezzature e esistenza di una istruzione per la corretta alimentazione e tenuta del registro.

Controlli e prescrizioni specifiche in materia di salute e sicurezza sul lavoro connessi alla stipula di un contratto di appalto e subappalto, d'opera o di somministrazione

I controlli di cui sopra possono essere di seguito declinati nello specifico:

1. Individuazione dell'impresa o del lavoratore autonomo candidati alla stipula del contratto di appalto (o somministrazione) o d'opera, in conformità con le procedure interne relative all'approvvigionamento e con i principi previsti nel presente Modello, come specificato all'interno del Capitolo 8.
2. Verifica dell'idoneità tecnico professionale:
Il datore di lavoro verifica l'idoneità tecnico-professionale delle imprese appaltatrici o dei lavoratori autonomi in relazione ai lavori da affidare in appalto o mediante contratto d'opera o di somministrazione. Fino alla data di entrata in vigore di un apposito decreto volto a disciplinare

dettagliatamente le modalità di verifica dell'idoneità tecnica e professionale, la verifica è eseguita attraverso le seguenti modalità:

- acquisizione del certificato di iscrizione alla camera di commercio, industria e artigianato;
- acquisizione dell'autocertificazione dell'impresa appaltatrice o dei lavoratori autonomi del possesso dei requisiti di idoneità tecnico-professionale, ai sensi dell'articolo 47 del D.P.R. 28 dicembre 2000, n. 445.

3. Con riferimento ai contratti di subappalto stipulati dall'appaltatore, i criteri e modalità di svolgimento dell'attività di verifica dell'idoneità tecnico-professionale già stabiliti per l'appaltatore devono essere estesi al subappaltatore.
4. Formalizzazione del contratto di appalto, d'opera o di somministrazione nelle seguenti modalità:
 - Ogni forma di collaborazione con imprese terze e con lavoratori autonomi (Appaltatori) è formalizzata in un contratto scritto che contiene apposita dichiarazione di conoscenza della normativa di cui al D.Lgs. 231/2001 e di impegno al suo rispetto.
 - Indicazione nel contratto di appalto o di somministrazione dei costi relativi alla sicurezza del lavoro⁽⁷⁾: ad esclusione dei contratti stipulati per le ipotesi di somministrazione di beni e servizi essenziali, ciascun contratto di appalto e di somministrazione, deve indicare specificamente i costi relativi alla sicurezza del lavoro con particolare riferimento a quelli propri connessi allo specifico appalto. A tali dati possono accedere, su richiesta, il rappresentante dei lavoratori per la sicurezza e gli organismi locali delle organizzazioni sindacali dei lavoratori comparativamente più rappresentative a livello nazionale.
 - Il Servizio di Prevenzione e Protezione effettua una verifica sulla correttezza e completezza formale del contratto, in particolare sulla sua conformità sostanziale con la normativa vigente in materia di salute e sicurezza.
 - Tutti contratti sono autorizzati e firmati in conformità con il sistema di deleghe e poteri di firma di CSI.
5. Laddove possibile, le disposizioni contenute nel precedente punto 4. devono trovare applicazione anche con riferimento ai contratti di subappalto stipulato dall'appaltatore.
6. Trasmissione da parte del Committente all'appaltatore, al subappaltatore, al lavoratore autonomo nonché al soggetto somministrante delle informazioni sui rischi specifici esistenti nell'ambiente in cui questi sono tenuti ad operare e sulle misure di prevenzione e di emergenza adottate in relazione all'attività del committente stesso⁽⁸⁾.
7. Attività di cooperazione e di coordinamento degli interventi volti ad eliminare i rischi da interferenza⁽⁹⁾. Il datore di lavoro committente, l'appaltatore [ivi compreso l'eventuale subappaltatore], l'impresa somministrante e il lavoratore autonomo sono tenuti a cooperare all'attuazione delle misure di prevenzione e protezione dai rischi sul lavoro incidenti sull'attività lavorativa oggetto dell'appalto o del contratto d'opera o di somministrazione. Detti soggetti coordinano gli interventi di protezione e prevenzione dai rischi cui sono esposti i lavoratori, informandosi reciprocamente anche al fine di eliminare rischi dovuti alle interferenze tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'opera complessiva.
8. Redazione del Documento Unico di Valutazione dei Rischi da Interferenza.⁽¹⁰⁾

Il datore di lavoro committente è tenuto a promuovere l'attività di cooperazione e coordinamento, elaborando un unico documento di valutazione dei rischi che indichi le misure adottate per eliminare o, ove ciò non è possibile, ridurre al minimo i rischi da interferenze [DUVRI].

E' stabilito che detto DUVRI abbia data certa e sia allegato al contratto di appalto o di opera.

⁷ Articolo 26, comma 5 del D.Lgs. 9 aprile 2008, n. 81.

⁸ Articolo 26, comma 1, lettera b) D.Lgs. 9 aprile 2008, n. 81.

⁹ Articolo 26, comma 2 D.Lgs. 9 aprile 2008, n. 81.

¹⁰ Articolo 26, comma 3 D.Lgs. 9 aprile 2008, n. 81.

Le disposizioni del presente comma non si applicano ai rischi specifici propri dell'attività delle imprese appaltatrici o dei singoli lavoratori autonomi.

9. Controllo formale circa le modalità di esecuzione del contratto di appalto [e subappalto], d'opera o di somministrazione.

Gli adeguamenti del sistema di controllo interno alle prescrizioni di cui al presente capitolo sono oggetto di uno specifico documento definito Executive Summary (di cui al Paragrafo 4.2.1. della Parte Generale); l'attuazione di dette misure è oggetto di costante verifica e monitoraggio da parte dell'OdV.

15.6 Gestione della sicurezza per conto di altre Divisioni di CSI in Italia

La procedura per l'esecuzione delle attività inerenti al sistema di gestione della sicurezza in supporto ad altre Divisioni di Credit Suisse in Italia, in coerenza con i principi di condotta e comportamento previsti ai paragrafi 13.4 e 13.5, deve prevedere:

- formalizzazione di accordi di servizio o contratti con la descrizione dei servizi offerti, modalità e tempistica di esecuzione per la corretta gestione del sistema di sicurezza;
- adeguato sistema di deleghe e procure opportunamente formalizzate;
- individuazione delle principali figure coinvolte nel modello di gestione della sicurezza (Datore di Lavoro, Delegato del Datore di Lavoro, RSPP, RLS)
- descrizione esaustiva, assegnazione in forma scritta di ruoli, compiti e mansioni e accettazione formale da parte dell'interessato

15.7 Controlli dell'Organismo di Vigilanza

L'Organismo di Vigilanza ha facoltà discrezionale di porre in essere le attività di controllo periodico sulle attività aziendali potenzialmente a rischio di commissione dei reati contrari alla sicurezza sul lavoro; tali controlli sono volti a verificare la corretta esplicazione delle regole definite nel Modello e, in particolare, delle procedure interne in essere.

A questo fine, l'Organismo di Vigilanza provvede a:

- **monitorare l'efficacia ed il rispetto delle procedure** specifiche volte alla prevenzione dei reati contrari alla sicurezza sul lavoro;
- **esaminare** eventuali **segnalazioni specifiche** provenienti dagli organi di controllo interno o da qualsiasi dipendente o soggetto esterno ed effettuare degli accertamenti ritenuti necessari od opportuni in conseguenza delle segnalazioni ricevute.
- monitorare il rispetto del Piano di Sorveglianza Sanitaria;
- verificare periodicamente il libro infortuni della Banca ed indagare le cause e la gestione di eventuali infortuni occorsi;
- monitorare l'efficacia dei controlli, effettuati dal Responsabile del Sistema di Prevenzione e Protezione per verificare la corretta implementazione del modello di gestione della salute e della sicurezza;
- sollecitare l'aggiornamento tempestivo del modello di gestione della salute e della sicurezza sulla base delle evoluzioni normative, ovvero alla luce delle risultanze delle riunioni periodiche sulla sicurezza;
- verificare la frequenza delle iniziative di formazione – informazione periodica relativamente ai reati legati alla sicurezza sul lavoro.

16 REATI DI CRIMINALITÀ INFORMATICA

16.1 Le fattispecie di reati di criminalità informatica

I reati presupposto contenuti nella presente Parte Speciale sono disciplinati dall'articolo 24 – bis del Decreto.

- **Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491-bis c.p.)** – Tale ipotesi di reato si configura nel caso in cui un rappresentante o un dipendente della Banca falsifichi un documento informatico pubblico o privato, avente efficacia probatoria. A tal fine, per “documento informatico” si intende la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti, con esclusione dunque dei programmi informatici. Ad esempio, un dirigente della Banca ruba la smart card necessaria per utilizzare la firma digitale “forte” di un amministratore delegato di un’azienda concorrente, al fine di modificare un documento informatico avente valore legale, laddove per firma digitale “forte” si intende la firma elettronica la cui provenienza e integrità è stata preventivamente certificata da un Ente certificatore legalmente autorizzato.
- **Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)** – Tale ipotesi di reato si configura nel caso in cui un rappresentante o un dipendente della Banca si introduca abusivamente in un sistema informatico o telematico protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo. A tal fine, per “sistema informatico” si intende qualsiasi apparecchiatura o rete di apparecchiature interconnesse o collegate, una o più delle quali, attraverso l’esecuzione di un programma per elaboratore, compiono l’elaborazione automatica di dati (si è ritenuto, ad es., che anche un semplice personal computer possa essere considerato un vero e proprio sistema, per la ricchezza dei dati contenuti). Ad esempio, un dipendente della società accede, anche indirettamente tramite un apposito programma (“spyware”), al computer di un’azienda concorrente al fine di visualizzare i termini dell’offerta che quest’ultima intende presentare ad una gara d’appalto alla quale anche la società intende partecipare.
- **Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.)** – Tale ipotesi di reato si configura nel caso in cui un rappresentante o un dipendente della Banca abusivamente si procuri, riproduca, diffonda, comunichi o consegna codici o parole chiave o altri mezzi idonei all’accesso a un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornisca indicazioni o istruzioni idonee al predetto scopo, al fine di procurare a sé o ad altri un profitto o di recare un danno ad altri. Ad esempio, un dipendente della Banca si procura un codice d’accesso (password, smart card, ecc.) idoneo ad introdursi da remoto nella rete aziendale di una società concorrente.
- **Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)** – Tale ipotesi di reato si configura nel caso in cui un rappresentante o un dipendente della Banca si procuri, diffonda, comunichi o consegna un programma informatico avente per scopo o per effetto di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero di favorire l’interruzione (totale o parziale) o l’alterazione del suo funzionamento. Ad esempio, un dipendente della Banca diffonde, all’interno del sistema informatico appartenente all’azienda concorrente, un programma virus contenuto in un supporto rimovibile (chiave USB, CD, DVD), o tramite posta elettronica, che diffondendosi e riproducendosi mina la funzionalità di detto sistema.
- **Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)** – Tale ipotesi di reato si configura nel caso in cui un rappresentante o un dipendente della Banca intercetti fraudolentemente comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le

impedisca o le interrompa. Il reato si configura altresì qualora si riveli, mediante qualsiasi mezzo di informazione al pubblico, il contenuto delle predette comunicazioni. Ad esempio, un dipendente della Banca invii continuamente messaggi di posta elettronica (spam) ad un'azienda concorrente al fine di rallentare o bloccare le loro reti e i loro servizi di posta elettronica.

- **Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)** – Tale ipotesi di reato si configura nel caso in cui un rappresentante o un dipendente della Banca installi apparecchiature atte ad intercettare, impedire, o interrompere comunicazioni relative a un sistema informatico o telematico ovvero intercorrenti tra più sistemi. Ad esempio, un dipendente della Banca installa in alcuni terminali aziendali di un competitor un software ("trojan horse" o "spyware") che contiene una scheda che consente di intercettare informazioni riservate utili per CSI.
- **Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)** – Tale ipotesi di reato si configura nel caso in cui un rappresentante o un dipendente della Banca distrugga, deteriori, cancelli, alteri o renda inservibili, anche parzialmente, informazioni, dati o programmi informatici altrui. Se il fatto è commesso con abuso della qualità di amministratore del sistema, costituisce una circostanza aggravante. Ad esempio, CSI assolda un hacker (o cracker) che modifica il sito web dell'azienda concorrente (cosiddetto "web defacing"), facendo apparire informazioni false o tali da compromettere la reputazione dell'azienda stessa.
- **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.)** – Tale ipotesi di reato si configura nel caso in cui un rappresentante o un dipendente della Banca distrugga, deteriori, cancelli o renda inservibili informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico, o comunque di pubblica utilità. Se il fatto è commesso con abuso della qualità di amministratore del sistema, costituisce una circostanza aggravante.
- **Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)** – Tale ipotesi di reato si configura nel caso in cui un rappresentante o un dipendente della Banca distrugga, danneggi, deteriori, o renda inservibili, anche parzialmente, sistemi informatici o telematici altrui. Se il fatto è commesso con abuso della qualità di amministratore del sistema, costituisce una circostanza aggravante. Ad esempio, un dipendente di CSI trasmette una e-mail contenente virus ai sistemi informatici appartenenti ad un'azienda concorrente, provocando un malfunzionamento dei sistemi informatici utilizzati dalla stessa azienda, paralizzandone l'attività lavorativa.
- **Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.)** – Tale ipotesi di reato si configura nel caso in cui un rappresentante o un dipendente della Banca distrugga, danneggi, deteriori, renda inservibili, anche parzialmente, i sistemi informatici o telematici di pubblica utilità, ovvero ne ostacoli il corretto funzionamento. Se il fatto è commesso con abuso della qualità di amministratore del sistema, costituisce una circostanza aggravante. Ad esempio, CSI inserisce dei virus nei sistemi informatici appartenenti alla società fornitrice di energia elettrica, provocando un malfunzionamento del sistema di rendicontazione dei Kw consumati da CSI stessa.
- **Frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.)** – Tale ipotesi di reato si configura nel caso in cui il soggetto che presta servizi di certificazione di firma elettronica violi gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri un danno. Trattandosi di un reato proprio, lo stesso sarà configurabile per CSI qualora la condotta venga posta in essere in concorso con il soggetto "che presta servizi di certificazione delle firme elettroniche". Ad esempio, un dipendente di CSI corrompe un certificatore al fine di ottenere un certificato in realtà appartenente ad una persona fittizia.

La persona fisica che commette un reato di criminalità informatica è punita con la reclusione da un minimo di sei mesi ad un massimo di otto anni e con una multa fino a 10.329 Euro.

Per la Società sono previste sanzioni pecuniarie da 100 a 500 quote (da 25,8 mila Euro a 774,5 mila Euro) e sanzioni interdittive ex art. 9, comma 2 del D.Lgs. 231/2001, per un periodo da tre mesi a due anni.

16.2 Processo di gestione della sicurezza informatica

Come descritto nella Parte Generale al Capitolo 4 dedicato alla descrizione dell'approccio metodologico adottato per l'aggiornamento del Modello, con specifico riferimento alle analisi e valutazioni condotte in materia di criminalità informatica, per sua natura tema pervasivo di diversi ambiti ed attività aziendale, l'attenzione è stata posta su quello che può essere definito quale il processo di "gestione della sicurezza informatica".

Il rischio di potenziale commissione dei reati in oggetto è per la natura stessa di tali fattispecie delittuose, potenzialmente "presente" in tutte le attività svolte dai dipendenti o da collaboratori a progetto/lavoratori interinali/somministrati della Banca che prevedono l'utilizzo dei sistemi e degli applicativi informatici (IT) di CSI.

In considerazione di quanto sopra esposto, possono essere ritenuti coinvolti nella gestione della sicurezza tutti i dipendenti, collaboratori a progetto, lavoratori interinali/somministrati ecc. a prescindere dalla loro collocazione, dalla forma della loro collaborazione con la società, dalle mansioni svolte e dal livello gerarchico, in quanto sono obbligati a svolgere le loro attività nel rispetto del sistema delle regole e norme di riferimento per l'utilizzo dell'IT.

Tuttavia, il rischio potenziale, in termini di probabilità di accadimento di uno dei reati in materia informatica e relative conseguenze, può essere valutato in correlazione alle caratteristiche delle attività svolte e ai sistemi IT utilizzati. In conseguenza di ciò, anche il sistema dei controlli adottato per mitigare il livello di rischio identificato presenta un livello di articolazione coerente con la natura e il livello potenziale del rischio specifico.

Le aree ritenute essere esposte ad un maggior rischio possono essere riconducibili a quelle a cui sono delegate compiti inerenti alcuni processi per la gestione della sicurezza informatica (autorizzazione accessi ai sistemi) e quelle in cui la frequenza, la complessità e la criticità nell'utilizzo dell'IT è maggiore e in cui le competenze informatiche dei soggetti coinvolti risultano più elevate.

16.3 Processi a Rischio

Il rischio di commissione dei reati in oggetto è potenzialmente presente in tutte le attività operative svolte dai dipendenti o da collaboratori all'interno della sede di CSI.

Tuttavia, possono essere considerate maggiormente sensibili al rischio, le funzioni specificatamente deputate al presidio della gestione del sistema di sicurezza informatica quali Information Technology e Human Resources.

	Direzione Executive Board Collegio Sindacale	Regional Management (BPPM e ORM)	PB: Canali distribuiti	Corporate Advisory	Advisory and Sales (AOF, Product and Services, Investment Consulting)	PB: FOS Casse	CP&D	AM: Canali distribuiti	AM: Portfolio Management and Product Control	Internal Audit	Direttore Compliance	Direttore Legal	Operations	Information Technology	Credit Manager	CRES - Immobili Servizi/Sicurezza e Prevenzione	Direttore Ufficio Acquisti - Supply Mgmt	Direttore Risorse Umane	Direttore Financial Accounting
REATI INFORMATICI	Falsità di documenti	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	SI	NO	NO	NO	NO
	Accesso abusivo ad un sistema informatico o telematico	SI	NO	SI	NO	NO	NO	SI	NO	NO	NO	NO	NO	NO	SI	NO	NO	NO	NO
	Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici	SI	NO	SI	NO	NO	NO	SI	NO	NO	NO	NO	NO	NO	SI	NO	NO	NO	NO
	Diffusione di apparecchiature, dispositivi o programmi informatici	SI	NO	SI	NO	NO	NO	SI	NO	NO	NO	NO	NO	NO	SI	NO	NO	NO	NO
	Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche	SI	NO	SI	NO	NO	NO	SI	NO	NO	NO	NO	NO	NO	SI	NO	NO	NO	NO
	Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche	SI	NO	SI	NO	NO	NO	SI	NO	NO	NO	NO	NO	NO	SI	NO	NO	NO	NO
	Danneggiamento di informazioni, dati e programmi informatici	SI	NO	SI	NO	NO	NO	SI	NO	NO	NO	NO	NO	NO	SI	NO	NO	NO	NO
	Danneggiamento di informazioni, dati e programmi informatici	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	SI	NO	NO	NO	NO
	Danneggiamento di sistemi informatici o telematici	SI	NO	SI	NO	NO	NO	SI	NO	NO	NO	NO	NO	NO	SI	NO	NO	NO	NO
	Danneggiamento di sistemi informatici o telematici di	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	SI	NO	NO	NO	NO
	Frode informatica del soggetto che presta servizi di certificazione di firma elettronica	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO

16.4 Principi generali di condotta e comportamento e di assetto del sistema di organizzazione, gestione e controllo

La presente sezione illustra i principi generali di condotta e comportamento, nonché di assetto del sistema di organizzazione, gestione e controllo che, unitamente ai principi specifici sanciti nel paragrafo 16.5 dovranno essere seguite dai Destinatari al fine di prevenire il verificarsi dei Reati descritti nel Paragrafo 16.1:

- a) CSI agisce nel rispetto della normativa vigente (tra cui la D.Lgs. 196/2003 “Codice in materia di protezione dei dati personali”), dotandosi e curando periodicamente l'aggiornamento di politiche e di procedure operative;
- b) CSI si impegna a mantenere la tracciabilità degli strumenti informatici – che rimangono di esclusiva proprietà dell'azienda - assegnati ai propri dipendenti e ne verifica preventivamente le caratteristiche tecniche, le configurazioni e gli accessi alla rete aziendale;
- c) l'utilizzo dei sistemi informatici da parte dei soggetti assegnatari dev'essere conforme alle politiche ed alle procedure adottate dall'azienda per assicurarne un adeguato livello di protezione;
- d) CSI assicura il corretto impiego e la regolare funzionalità della posta elettronica e della rete *internet* definendo le modalità d'uso consentite nello svolgimento dell'attività lavorativa;
- e) i dati, le informazioni ed i documenti dei quali si viene a conoscenza nello svolgimento delle proprie mansioni, devono essere utilizzati esclusivamente per motivi di ufficio e gestiti nel rispetto delle politiche e delle procedure aziendali, nonché delle deleghe e delle procure, volte ad assicurare un'adeguata gestione e protezione degli stessi;
- f) le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità Pubbliche di Vigilanza (Consob, Borsa Italiana SpA, Garante della Privacy, ecc.) devono essere effettuate nel rispetto dei seguenti presidi specifici:
 - segregazione delle attività;
 - deleghe e procure;
 - norme/ procedure/circolari interne esistenti;
 - tracciabilità dei soggetti che producono l'informazione e di chi effettua la trasmissione dei dati.

In particolare, tutti i dipendenti e collaboratori di CSI sono tenuti a:

- astenersi dal tenere comportamenti tali integrare le fattispecie previste dai suddetti reati di criminalità informatica, ovvero da comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possono potenzialmente diventarlo;
- rispettare le regole di condotta generale, i principi di controllo e le prescrizioni specifiche formulate nel presente Modello;
- rispettare le norme, le policy e le procedure aziendali che disciplinano l'accesso e l'utilizzo dei sistemi e degli applicativi informatici di CSI;
- promuovere il rispetto delle suddette norme, regole e principi.

16.5 Procedure Specifiche**16.5.1 Gestione della sicurezza dei sistemi informatici e dei dati**

Esistenza e diffusione di disposizioni organizzative e di un sistema formalizzato di ruoli, poteri e deleghe con riferimento al processo di gestione della sicurezza informatica, in particolare:

- la definizione dei ruoli e delle responsabilità in tema di sicurezza informatica è inclusa nelle descrizioni delle attività del personale (job description), dove applicabile, e adeguatamente formalizzata, con l'identificazione dell'organizzazione, ruoli e responsabilità;
- l'identificazione del Responsabile della Sicurezza Informatica avviene sulla base di una specifica e formalizzata disposizione organizzativa.

Esistenza di policy, procedure e disposizioni operative formalizzate che disciplinano le attività dei soggetti coinvolti nel processo di gestione della sicurezza informatica, in particolare:

- Esistenza di una “Policy relativa alla Sicurezza Informatica”, diffusa a tutta l’organizzazione, che stabilisce i principi aziendali sulla sicurezza del patrimonio informativo. Tale documento contiene le seguenti linee guida:
 - una definizione di Sicurezza Informatica e la sua importanza come fattore abilitante dello scambio delle informazioni all’interno e all’esterno dell’azienda;
 - le direttive della Direzione e le sue intenzioni, che promuovono gli obiettivi e i principi della sicurezza del sistema informativo;
 - una descrizione delle politiche di sicurezza aziendali specifiche, i principi, gli standard e i requisiti, comprendendo:
 - Aderenza alle leggi, regolamenti e obblighi contrattuali,
 - Requisiti circa la formazione specifica sulla sicurezza,
 - Politica di prevenzione e rilevazione dei virus,
 - Politiche di Business Continuity Planning.
 - una definizione delle responsabilità generali del management e di quelle specifiche riguardanti la sicurezza informatica;
 - una spiegazione del processo di rilevazione e segnalazione dei casi di effettivo e sospetto incidente sulla sicurezza.
- Esistenza e aggiornamento periodico del Documento Programmatico sulla Sicurezza dei dati conformemente a quanto disposto dal D.Lgs. n. 196 del 30 giugno 2003;
- Esistenza di una procedura diretta alla gestione e controllo dei dati e dei documenti che contenga:
 - l’individuazione dei requisiti di sicurezza;
 - il periodico riesame, la modifica o integrazione;
 - la disponibilità presso il luogo di lavoro e la diffusione a tutti gli interessati;
 - la sostituzione o distruzione di tutti i documenti e le informazioni superate od obsolete;
 - la prescrizione che imponga che i documenti siano archiviati e i dati conservati ai fini legali e/o per finalità gestionali o operative.
- Esistenza di una procedura di classificazione di tutti i sistemi informatici (elaboratori, terminali, strumenti di rete, accessori, ecc.) finalizzata a definire le linee guida per le nuove acquisizioni. La procedura deve comprendere una parte relativa alle responsabilità del gruppo sicurezza informatica che partecipa alla definizione delle nuove tecnologie e relative acquisizioni.
- Esistenza di procedure formalizzate, estese e diffuse a tutto il personale, per la rilevazione la tempestiva segnalazione degli incidenti sulla sicurezza. Tale procedura deve indicare le azioni da compiere e la condotta da seguire, le persone o funzioni aziendali da contattare e le modalità di segnalazione degli incidenti di cui si è stati testimoni. Le procedure devono inoltre consentire di adottare le azioni correttive adeguate tempestivamente e organizzare un archivio storico, utile a fine di prevenzione e di adozione di nuove contromisure.
- Esistenza di policy e procedure aziendali che formalizzino le modalità di profilazione delle utenze e l’utilizzo delle risorse informatiche aziendali.
- Esistenza di policy e procedure aziendali che formalizzino i criteri e le modalità di accesso e utilizzo dei sistemi informatici aziendali.
- Esistenza di procedure formalizzate di sicurezza che siano volte a prevenire i rischi dovuti alle connessioni esistenti con le terze parti.
- Esistenza di una politica di gestione della sicurezza degli apparati quando non sono presidiati. Deve inoltre essere stabilita una politica per la disconnessione dalla rete da parte degli utenti che non svolgono attività da un certo periodo di tempo. Tale politica deve anche comprendere i criteri per definire le eventuali restrizioni ai tempi e alla durata delle connessioni quando riguardano applicazioni critiche.

Accesso e utilizzo dei sistemi informatici:

- L’accesso ai sistemi e applicativi informatici avviene sulla base di un’opportuna profilazione degli utenti;

- I criteri con cui si assegnano i privilegi ed i diritti di accesso alle risorse informatiche e ai dati devono essere determinati sulla base dell'analisi delle effettive necessità, connesse al tipo di incarico svolto. Deve inoltre essere prevista una revisione periodica dei privilegi concessi.
- La revisione delle condizioni che hanno portato a concedere i vari privilegi di accesso deve costituire un processo continuo e formalizzato e deve avvenire nel rispetto dei seguenti principi:
 - revisione dei diritti di accesso degli utenti ad intervalli regolari;
 - revisione delle autorizzazioni per gli account privilegiati (amministratori di sistema, ecc.) ad intervalli più frequenti;
 - controllo della distribuzione dei privilegi a intervalli regolari finalizzati a garantire che utenti non autorizzati abbiano ottenuto privilegi non di loro spettanza;
 - rispetto del principio generale del "need-to-know" (ognuno deve avere accesso solo ai dati e applicazioni di propria competenza e necessari per lo svolgimento delle proprie mansioni)
- l'accesso ai sistemi e applicativi informatici è consentito tramite un sistema di protezione che identifica ed autentica univocamente gli utenti, basato anche sull'utilizzo di *password* di accesso, nel rispetto dei seguenti requisiti:
 - assegnazione di una *password* per ciascun sistema informatico (es: rete aziendale, casella di posta elettronica, ecc)
 - la *password* è composta da un minimo di otto caratteri e possiede le caratteristiche previste dal D.Lgs. n. 196/2003 (Codice sulla Privacy)
 - la *password* è modificata dall'utente al primo utilizzo e, successivamente, con cadenza periodica (confronta il "*Disciplinare Tecnico in materia di misure minime di sicurezza*")
 - la *password* è strettamente *personale* e non può essere comunicata o condivisa con altri utenti aziendali, salvo espressa autorizzazione del Responsabile della sicurezza informatica.

Protezione fisica delle aree, dei locali server e delle postazioni di lavoro:

- L'installazione di nuove apparecchiature IT, strutture e procedure deve essere formalmente approvata. L'approvazione deve includere il parere favorevole del Responsabile della Sicurezza Informatica.
- Il processo di definizione ed approvazione di nuove strutture IT, e della loro modifica, deve essere sempre formalizzato. Il processo di approvazione comprende un'analisi, effettuata dal settore aziendale sulla sicurezza informatica, avente come finalità quella di assicurare che le nuove tecnologie non presentino lacune sotto il profilo della sicurezza e non influenzino negativamente i sistemi e le procedure attualmente presenti.
- l'installazione, l'utilizzo e la rimozione di apparecchiature e supporti rimovibili (*pendrive* USB, *CD-Rom*, ecc.) è consentito solo previa specifica autorizzazione da ottenre tramite apposito tool autorizzativo (MyAccess)
- i locali *server* devono essere adeguatamente individuati e protetti: l'accesso deve essere consentito solo a personale autorizzato tramite apposito dispositivo elettronico (badge), che consente la registrazione puntuale degli accessi.

Monitoraggio, controllo continuo e tracciabilità:

- Le Funzioni aziendali che sovrintendono alla sicurezza informatica devono essere informate in merito a segnalazioni di problemi ai programmi elaborativi, per verificare che la sicurezza del patrimonio informativo non sia stata pregiudicata;
- L'attività degli operatori del sistema informatico deve essere documentata per ottenere dati statistici circa l'occorrenza e la frequenza di determinati problemi, le migliori azioni da adottare e la pianificazione futura delle risorse informatiche;
- Gli addetti alla gestione operativa dei sistemi devono compilare un registro delle attività svolte. I problemi e gli errori riscontrati devono essere annotati insieme alle azioni correttive effettuate;

- Le attività svolte sui sistemi e sugli applicativi informatici devono essere tracciate attraverso adeguati “log” che consentano di ricostruire gli eventi e le operazioni effettuate e dei soggetti/utenti che le hanno poste in essere.

Altri controlli in materia di sicurezza informatica

Nella gestione e protezione delle reti e dei dati, si rende necessario che:

- gli utenti, nelle attività di salvataggio dei dati, rispettino le linee guida indicate dal Responsabile della Funzione IT e le procedure operative aziendali
- siano definite ed applicate procedure di controllo sullo stato di funzionamento e di obsolescenza delle apparecchiature hardware, dei software e delle applicazioni installate sulle stesse;
- tutte le informazioni aziendali che risiedono sui server e sulle banche dati centrali, siano sottoposte a regolare procedura di backup
- tutti i server e le postazioni di lavoro aziendali siano protetti da programmi antivirus, aggiornati automaticamente, contro il rischio di tentativi di intrusione dall'esterno;
- deve essere previsto un “Piano di Continuità Operativa” (c.d. Piano di Business Continuity) finalizzato a garantire l'integrità e la disponibilità dei dati e delle informazioni in ogni circostanza, che individui:
 - gli eventi che potrebbero causare crash di sistema;
 - i ruoli e le responsabilità dei soggetti coinvolti nell'esecuzione della procedura;
 - sito/i di backup dal/i quale/i è possibile effettuare le operazioni di ripristino delle funzioni e dei dati;
 - la successione delle azioni da implementare per ripristinare le funzioni ed i dati;
- deve essere previsto nei contratti con terze parti l'introduzione di specifiche clausole a previsione delle politiche e procedure di sicurezza informatica volte a prevenire i rischi dovuti alle connessioni esistenti con i loro sistemi;

16.5.2 Trasmissione di dati, informazioni e documenti:

- la trasmissione di *files*, documenti, o qualsiasi altra documentazione di proprietà di CSI o di altra società del gruppo, deve essere effettuata per finalità strettamente attinenti allo svolgimento delle proprie mansioni, nei limiti delle deleghe e delle procure conferite, ed in conformità ai requisiti richiesti da prassi e procedure aziendali (sono previste, ad esempio, modalità specifiche per la trasmissione all'esterno di documenti/files classificati “secret” o “confidential”, che consentono la trasmissione sicura e la tracciabilità dei flussi in uscita);
- il sistema di protezione deve essere in grado di identificare univocamente gli utenti che accedono ad un sistema trasmissivo e di tracciare i dati ed i documenti trasmessi all'esterno;

16.5.3 Gestione del personale

La procedura di **gestione del personale** deve garantire che:

- al momento dell'ingresso in azienda di un nuovo dipendente il Responsabile della Funzione Personale provveda all'assegnazione di un codice univoco di identificazione del dipendente che consente l'avvio del work-flow autorizzativo (tramite il tool MyAccess) per la richiesta alla Funzione IT degli strumenti e supporti informatici propedeutici allo svolgimento delle mansioni e l'elenco degli applicativi per i quali è necessario fornire l'accesso al nuovo dipendente;
- il Responsabile della Funzione IT consegni ad ogni nuovo dipendente:
 - i dispositivi *hardware* (*pc*, *notebook*, etc.) correttamente configurati con i programmi *software* necessari all'espletamento delle mansioni assegnate;
 - le *passwords* iniziali di accesso ai sistemi informatici di elaborazione ed eventualmente di trasmissione dati all'esterno, che dovranno essere tempestivamente personalizzate dal singolo utente;
- la Società attui una politica di formazione e/o di comunicazione inerente alla sicurezza dei sistemi informatici e dei dati, volta a sensibilizzare tutti gli utenti.

Gli adeguamenti del sistema di controllo interno alle prescrizioni di cui al presente capitolo sono oggetto di uno specifico documento definito Action Plan, la cui attuazione è oggetto di costante verifica e monitoraggio da parte dell'OdV.

16.6 Controlli dell'Organismo di Vigilanza

Con riferimento ai processi a rischio identificati nella presente sezione, l'Organismo di Vigilanza ha il compito di verificare:

- l'adozione ed il periodico aggiornamento da parte di CSI di procedure operative e regolamenti interni relativi alla sicurezza dei sistemi informatici e dei dati, opportunamente diffusi e rispettati dai dipendenti;
- il corretto funzionamento dei processi di autenticazione e di accesso ai sistemi informatici ed ai dati;
- che la Società abbia, nei termini di legge, aggiornato il Documento Programmatico sulla Sicurezza dei dati (ex D.Lgs. 196/2003);
- l'efficacia ed il rispetto delle procedure previste per la protezione delle reti;
- la corretta implementazione ed il rispetto delle procedure previste per la protezione ed il salvataggio dei dati (procedure di *backup*, *disaster recovery*);
- l'adeguatezza e la puntuale implementazione delle procedure previste per la protezione delle aree, dei locali *server* e delle postazioni di lavoro;
- il corretto svolgimento dei processi di trasmissione dei dati, informazioni e documenti all'esterno dell'azienda;
- l'osservanza della procedura relativa alla consegna di strumenti, supporti informatici e credenziali di accesso ai dipendenti.

17 REATI DI RICICLAGGIO

17.1 Le fattispecie di reati di ricettazione, riciclaggio, impiego di denaro, beni ed utilità di provenienza illecita e autoriciclaggio

L'art. 63 del D.Lgs. 231/2007, "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", ha introdotto l'art. 25-octies del D.Lgs. 231/2001, che richiama i seguenti articoli del codice penale:

- **Ricettazione (art. 648 c.p.)** – Tale ipotesi di reato si configura nel caso in cui taluno acquisti o riceva o occulti denaro o cose provenienti da un qualsiasi delitto al fine di procurare a sé o ad altri un profitto. Ad esempio qualora il dirigente della società incaricato di selezionare i fornitori e acquistare dell'hardware per CSI, acquisti tali beni sotto costo perché proveniente da un illecito (ad es. furto), con profitto per CSI.
- **Riciclaggio (art. 648 bis c.p.)** – Tale ipotesi di reato si configura nel caso in cui taluno sostituisca o trasferisca denaro o beni provenienti da delitto non colposo ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa; ad esempio qualora il dirigente di CSI versi quale corrispettivo per un Consulente somme di denaro che sa provenire da un delitto commesso da un cliente, al fine di occultare tale provenienza
- **Impiego di denaro, beni o utilità di provenienza illecita (648-ter c.p.)** – Tale ipotesi di reato si configura nel caso in cui taluno impieghi in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto; ad esempio qualora un dirigente della società utilizzi per attività pubblicitarie di CSI somme di denaro ricevute da un cliente, sapendo che tale somme provengono da delitto.

L'art. 64, comma 1, lett. f) abroga i commi 5 e 6 dell'art. 10 della l. n. 146/2006, di contrasto al crimine organizzato transnazionale, con la conseguenza che la commissione dei reati di cui agli artt. 648, 648 bis e 648 ter del c.p., diventa causa di responsabilità ex D.Lgs. n. 231/2001 anche nei casi in cui tali reati non si configurino come transnazionali.

Tali reati pertanto rientrano nella categoria dei reati di riciclaggio e non più in quella dei reati transnazionali.

La L. n. 186/2014, in vigore dal 1 gennaio 2015, ha inserito all'art. 25-octies D.Lgs. 231/2001 il reato di autoriciclaggio, punito dall'art. 648-ter.1 c.p.:

- **Autoriciclaggio (art. 648-ter.1 c.p.)** - Tale ipotesi di reato si configura nei confronti di chiunque, avendo commesso o concorso a commettere un delitto non colposo, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

La persona fisica che commette un reato di riciclaggio è punita con la reclusione da un minimo di due ad undi dodici anni e con una multa da 516,46 Euro fino a 25.000 Euro.

Per la Società sono previste sanzioni pecuniarie da 200 a 1000 quote (da 51,6 mila Euro a 1.549 mila Euro) e sanzioni interdittive per un periodo non inferiore a due anni.

Oggetto Materiale dei reati:

L'oggetto materiale dei reati sopra descritti può essere costituito da qualsiasi entità economicamente apprezzabile e possibile oggetto di scambio, quale il denaro, i titoli di credito, i

mezzi di pagamento, i diritti di credito, i preziosi, i beni materiali ed immateriali in genere. Deve però trattarsi di bene o utilità proveniente da delitto, vale a dire esso ne deve costituire il prodotto (risultato, frutto ottenuto dal colpevole con la commissione del reato), il profitto (lucro o vantaggio economico ricavato dal reato) o il prezzo (compenso dato per indurre, istigare, determinare taluno alla commissione del reato).

Inoltre, l'art. 2 del D.Lgs 231/07. precisa che il riciclaggio è considerato tale anche se le attività, che hanno generato i beni da riciclare, si siano svolte nel territorio di un altro Stato comunitario o di un Paese terzo.

La Funzione Antiriciclaggio e il Responsabile Antiriciclaggio

Il *“Provvedimento recante disposizioni attuative in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari e degli altri soggetti che svolgono attività finanziaria ai fini di riciclaggio e di finanziamento del terrorismo, a norma dell'art. 7, comma 2, del d. lgs. 231/2007”* dispone che, a partire dal 1° settembre 2011 i destinatari della normativa implementino una specifica funzione antiriciclaggio indipendente e dotata di risorse adeguate, specificando i compiti che dovranno essere svolti da tale funzione.

I destinatari valutano gli assetti strutturali ed organizzativi della funzione tenendo in considerazione la propria organizzazione, attività, clientela, prodotti e propensione al rischio. La funzione può essere costituita in modo autonomo oppure nell'ambito di strutture organizzative diverse, quali la Compliance, o il Risk Management (è esclusa l'assegnazione alla funzione di revisione interna) oppure può essere esternalizzata, purché il processo di gestione dei rischi sia ricondotto ad unità mediante la nomina di un Responsabile con compiti di coordinamento e di supervisione. In caso di esternalizzazione, la responsabilità rimane comunque in capo al destinatario.

Alla funzione sono assegnati compiti specifici quali:

- identificare le norme applicabili, valutarne l'impatto e collaborare alla individuazione degli assetti organizzativi per la prevenzione del rischio riciclaggio, proponendo modifiche organizzative e procedurali per il presidio di tale rischio;
- dare consulenza e assistenza agli organi aziendali, curando l'attività di formazione, in sinergia con gli altri organismi competenti;
- verificare l'effettiva applicazione dei controlli previsti sulle procedure, svolgendo, altresì, le attività di “verifica rafforzata” sulla clientela, che presenta livelli di rischio-riciclaggio più elevati;
- predisporre flussi informativi verso gli organi aziendali e l'alta direzione: in tal senso, almeno una volta l'anno, la funzione presenta una relazione sulle iniziative intraprese, sulle disfunzioni accertate e sulle relative azioni correttive da intraprendere nonché sull'attività informativa;
- predisporre un documento, da sottoporre all'approvazione del vertice dell'impresa, che definisce compiti e modalità operative nella gestione del rischio-riciclaggio e di finanziamento del terrorismo (documento da aggiornare e da rendere disponibile a tutto il personale dipendente e ai collaboratori).

Rilievo particolare assume la figura del *Responsabile della funzione antiriciclaggio* che si colloca tra i responsabili di funzioni aziendali di controllo e che deve essere in possesso di requisiti di indipendenza, autorevolezza e professionalità.

In particolare, la normativa prevede che il Responsabile non debba avere responsabilità dirette di aree operative o essere gerarchicamente dipendente da soggetti responsabili di tali aree.

E' richiesta anche la nomina della figura di Responsabile o, in sua vece, di Delegato alla segnalazione delle operazioni sospette, il cui nominativo va comunicato all'UIF. La delega può essere attribuita al Responsabile antiriciclaggio, ma non oggetto di esternalizzazione.

17.2 Processi/Aree rischio e BU coinvolte

In considerazione della struttura e delle attività svolte la Banca, tramite l'attività di control and risk self assessment condotta (cfr. capitolo 4.2.1 "Approccio metodologico"), ha individuato i seguenti Processi/Aree a rischio con riferimento ai reati di riciclaggio, ricettazione e impiego di denaro, beni o utilità di provenienza illecita:

- *gestione amministrativa clienti;*
- *servizi bancari: gestione della liquidità, dei bonifici e dei crediti;*
- *gestione fornitori e acquisti di beni e servizi;*
- *gestione del personale, degli agenti e dei promotori finanziari.*

La normativa in materia di contrasto del riciclaggio e finanziamento del terrorismo ha un approccio di tipo preventivo e richiede l'adozione di una serie di presidi e regole al fine di conformarsi alle disposizioni in materia di:

- limitazione all'uso del contante e dei titoli al portatore;
- obblighi di adeguata verifica del cliente;
- obblighi di registrazione e tenuta dell'AUI
- obblighi di segnalazione delle operazioni sospette.

Sulla base delle analisi effettuate sulla struttura aziendale, il rischio che si verifichino i reati di ricettazione, riciclaggio e impiego di denaro, beni e utilità di provenienza illecita nel contesto di CSI appare, più marcato, quale rischio tipico del circuito bancario e finanziario, principalmente con riferimento ai rapporti con la clientela, ed in particolare per quanto concerne l'instaurazione e la gestione dei rapporti continuativi. Altre funzioni aziendali, strumentali alla commissione dei reati in oggetto, sono state individuate e rappresentate nella tabella di sintesi qui di seguito:

		Direzione Executive Board Collegio Sindacale	Regional Management (BPPM e ORM)	PB: Canali distribuiti	Corporate Advisory	Advisory and Sales (AOF, Product and Services, Investment Consulting)	PB: FOS Casse	CP&D	AM: Canali distribuiti	AM: Portfolio Management and Product Control	Internal Audit	Direttore Compliance	Direttore Legal	Operations	Information Technology	Credit Manager	CRES - Immobili Servizi/Sicurezza e Prevenzione	Direttore Ufficio Acquisti - Supply Mgmt	Direttore Risorse Umane	Direttore Financial Accounting
REATI DI RICICLAGGIO	Ricettazione	SI	NO	SI	NO	NO	SI	NO	SI	NO	NO	NO	NO	NO	NO	NO	SI	SI	NO	NO
	Riciclaggio	SI	NO	SI	SI	NO	SI	NO	SI	NO	NO	NO	NO	SI	NO	SI	NO	SI	NO	NO
	Impiego di denaro, beni o altra utilità di provenienza illecita	SI	NO	SI	NO	NO	SI	NO	SI	NO	NO	NO	NO	NO	NO	NO	SI	SI	NO	NO

Con specifico riferimento al reato di autoriciclaggio (art. 648-ter.1 c.p.), introdotto tra i reati societari di cui all'art. 25-octies D.Lgs. 231/2001 dalla Legge 186/2014, nel corso delle attività di control and risk self assessment condotte nel 2015 sono stati individuati i seguenti ambiti di attività potenzialmente a rischio 231 (identificati anche come Processi/Aree a rischio):

- *gestione delle attività di distribuzione e negoziazione con riferimento ai clienti "istituzionali": fondi pensione (occupazionali e pre-esistenti), casse di previdenza, compagnie di assicurazione, fondazioni bancarie;*
- *gestione delle attività di sviluppo commerciale per la distribuzione di prodotti Credit Suisse nei canali Retail e Wholesale;*
- *gestione delle attività di marketing per la Divisione Asset Management (selezione, negoziazione, formalizzazione, pagamento);*
- *attività di origination e negoziazione dei contratti con la clientela "Private Banking" per i servizi di consulenza e gestione (suddivisi in relazione alla segmentazione della tipologia clientela target: imprenditori, UHNWI...);*
- *gestione della vendita di prodotti strutturati alla Clientela Professional;*
- *gestione dei segnalatori (selezione, contrattualizzazione, pagamento);*
- *attività di origination e negoziazione dei servizi di corporate advisory;*
- *fatturazione dei servizi di corporate advisory;*
- *gestione degli agenti (selezione, contrattualizzazione, ecc.);*
- *gestione del sistema di remunerazione e incentivazione dei banker (dipendenti);*
- *gestione del sistema di remunerazione e incentivazione degli agenti;*
- *amministrazione e gestione del personale (Elaborazione ed erogazioni paghe, ecc.);*
- *gestione delle attività di marketing per la Divisione Private Banking (gestione ed organizzazione eventi, predisposizione di strumenti e materiale di comunicazione a supporto della funzione commerciale);*
- *attività di origination, negoziazione, erogazione e back-office relative alla sottoscrizione e gestione dei contratti relativi a prodotti creditizi (Lombard, anticipazioni fondiari, mutui, operazioni creditizie "Strutturate");*
- *gestione della fiscalità (attività c.d. "new business" e consulenza);*
- *gestione della fiscalità (adempimenti fiscali).*

Nella tabella di sintesi sono indicate le Business Unit a cui fanno capo la gestione e il governo dei Processi/Aree a rischio sopra indicati:

		Desk imprendi tori	Corporat e Advisory	PB COO	PB HEAD	Business Risk Manager	Marketin g strategico	Products	Internal Audit	CRO Operatio nal Risk Manager	FOS / MIDDLE OFFICE	Distributi on	AM COO	Credit Risk Manage ment / Credit Consulta nt	TAX	Front Office	Business Process & Risk	HR
AUTORICICLAGGIO	Autoriciclaggio	SI	SI	SI	SI	NO	SI	NO	NO	NO	NO	SI	NO	SI	NO	NO	NO	SI

17.3 Principi di controllo e di comportamento ed assetto del sistema di organizzazione, gestione e controllo

Si riporta di seguito il protocollo che detta i principi di controllo e i principi di comportamento applicabili alla gestione dei rischi in materia di contrasto al riciclaggio dei proventi di attività criminali ed al finanziamento del terrorismo. Tali principi si completano con la normativa aziendale di dettaglio che regola l'attività medesima.

In particolare, con riferimento alle aree a rischio devono essere adottate, le seguenti procedure e regole di condotta:

- devono essere rispettate le Direttive e Procedure adottate in ottemperanza al D.Lgs. 231/2007 in materia di antiriciclaggio, e quelle poste in essere in base alle "Istruzioni operative per l'individuazione di operazioni sospette" della Banca d'Italia;
- in particolare si devono tenere dei comportamenti conformi alle prescrizioni contenute nel "Manuale Antiriciclaggio" che illustra a tutto il personale di Credit Suisse in Italia le principali regole dettate dalla normativa antiriciclaggio italiana;
- devono essere inoltre seguite tutte le regole in essere a livello di Gruppo in materia di antiriciclaggio, con particolare riferimento alla Compliance Policy Anti-Money Laundering.

In linea generale gli aspetti caratterizzanti le Direttive e Procedure in materia di antiriciclaggio vigenti a livello locale e di Gruppo possono essere riconducibili ai seguenti elementi:

1. identificazione di ogni cliente, incluso l'eventuale titolare effettivo;
2. indicazione del "quando" (es. instaurazione di un rapporto continuativo, esecuzione di un'operazione occasionale di importo superiore alle soglie stabilite per legge, ecc...) e del "come" (es. modalità di identificazione del cliente, del titolare effettivo, di scopo e natura delle transazioni, ecc...) adempiere a tali obblighi;
3. definizione di un approccio basato sul rischio, per cui gli obblighi di adeguata verifica della clientela si articolano in differenti gradi di *due diligence* commisurati al profilo di rischio del cliente (es. obblighi semplificati per Intermediari Finanziari e per Uffici della Pubblica Amministrazione, e obblighi rafforzati per clienti non fisicamente presenti all'instaurazione del rapporto, per soggetti politicamente esposti – PEP¹¹ – non residenti, per enti corrispondenti extracomunitari, per clientela con profilo di rischio riciclaggio massimo, ecc.);
4. monitoraggio dell'attività svolta da ogni cliente, in particolare:
 - monitoraggio nel medio-lungo periodo da parte delle Strutture Aree/Funzioni/Uffici/Strutture organizzative preposte che garantisca un controllo incrociato tra il profilo soggettivo del cliente, la tipologia di operazione, la frequenza e le modalità di esecuzione, l'area geografica di riferimento (con particolare riguardo all'operatività da/verso Paesi a rischio) e ancora il grado di rischio attribuito al prodotto oggetto dell'operazione, i fondi impiegati, l'orizzonte temporale dell'investimento, il comportamento tenuto dal cliente al momento dell'esecuzione dell'operazione (qualora venga eseguita in presenza del cliente);
 - monitoraggio e presidio da parte delle Strutture preposte al controllo interno della puntuale esecuzione nel pieno rispetto dei termini e delle disposizioni di legge e della normativa interna, delle attività delle Strutture operative;
 - rilevazione e valutazione degli altri indici di anomalia eventualmente presenti nella concreta operatività;
 - rilevazione delle infrazioni delle disposizioni in tema di limitazioni nell'utilizzo del contante e dei titoli al portatore;

¹¹ L'acronimo PEP sta per Politically Exposed Person o, in italiano, persona politicamente esposta. Per la definizione di PEP fare riferimento all'art. 1, comma 2 lettera o) del D. Lgs. n. 231/2007 e all'art. 1 dell'Allegato Tecnico al D. Lgs. n. 231/2007.

- registrazione dei rapporti e delle operazioni nell' Archivio Unico Informatico (AUI) e conservazione dei documenti e delle informazioni, secondo quanto stabilito dall'Allegato tecnico di UIF
- 5. identificazione e comunicazione di comportamenti sospetti o inconsueti che possano nascondere attività di riciclaggio tutti i rapporti continuativi e le operazioni che comportano la trasmissione di mezzi di pagamento devono essere processati 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. Un archivio ordinato consente, infatti, tra l'altro, di evadere prontamente le richieste di informazioni da parte delle competenti Autorità e di ricostruire l'operatività della clientela anche a fini di monitoraggio e della corretta definizione del profilo di rischio: a tale fine è indispensabile procedere alle attività di "integrazione" e "sistemazione" delle operazioni o dei rapporti in stato di "sospeso" entro i termini consentiti dalle procedure e comunque nei termini previsti dalla norma;
- 6. i dipendenti ricevono un'adeguata informativa per permettere loro di conoscere gli obblighi, i rischi e le responsabilità connesse alla corretta applicazione delle policies antiriciclaggio
- 7. obbligo di astensione dall'apertura di un nuovo rapporto o dal mantenimento di un rapporto in essere nel caso in cui l'operatore non sia in grado di adempiere correttamente agli obblighi di adeguata verifica o sussista il sospetto che vi sia una relazione con il riciclaggio o con il finanziamento del terrorismo;
- 8. la designazione di un Money Laundering Prevention and Reporting (MLRO - Responsabile Antiriciclaggio); qualora il MLRO ricopra il ruolo di Delegato alla segnalazione di operazioni sospette ex art. 42 del D.Lgs. 231/07, deve essere formalmente incaricato ed il nominativo segnalato alla UIF;
- 9. obbligo di segnalazione delle operazioni sospette secondo gli indicatori di anomalia che devono essere oggetto di costante formazione del personale addetto e l'obbligo di comunicazione delle infrazioni alle disposizioni in tema di limitazioni per l'utilizzo del contante e dei titoli al portatore;
- 10. l'obbligo di registrazione nell'Archivio Unico Informatico (AUI) dei rapporti, dei dati identificativi e delle operazioni poste in essere dalla clientela;
- 11. monitoraggio di tutte le transazioni realizzate con Paesi che minacciano la pace e la sicurezza internazionale (Paesi inseriti nelle *sanction list*¹²);
- 12. adozione di adeguate misure di formazione del personale per garantire il corretto recepimento delle disposizioni normative e la loro corretta applicazione;
- 13. obbligo, posto a carico del Consiglio di Amministrazione, dell'Organismo di Vigilanza ai sensi del D. Lgs. n. 231/2001 e degli altri Organi di Controllo di adempiere a quanto previsto dall'art. 52 d.lgs 231/07 (obblighi di impulso e supplenza)
- 14. possibilità di assicurare la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate (in particolare l'Unità Organizzativa di volta in volta interessata 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 del processo);
- 15. riservatezza delle informazioni, con particolare riguardo a quelle relative all'individuazione dei titolari effettivi, alla profilatura dei clienti ed ai processi di monitoraggio delle operazioni e di segnalazione delle operazioni sospette, mediante l'adozione di idonee misure informatiche e fisiche;
- 16. sistematica erogazione di attività formative specificamente dedicate ai profili di rischio legati alla normativa antiriciclaggio.

¹²Al fine di prevenire l'insorgere di potenziali minacce, i Governi e le Organizzazioni Internazionali stilano specifiche liste – *sanction list* – di determinati Paesi, soggetti ed entità le cui attività divengono soggette a controllo e monitoraggio da parte delle Istituzioni Finanziarie. Tali liste sono definite ed aggiornate da Istituzioni quali le Nazioni Unite (NU), l'Unione Europea (UE), le banche centrali e, per gli Stati Uniti, l'Office of Foreign Assets Control (OFAC).

In ogni caso è **fatto divieto** di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D.Lgs. 231/2001 e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- instaurare rapporti continuativi, o mantenere in essere quelli preesistenti, ed eseguire operazioni quando non è possibile attuare gli obblighi di adeguata verifica nei confronti del cliente, ad esempio per il rifiuto del cliente a fornire le informazioni richieste;
- eseguire le operazioni per le quali si sospetta vi sia una relazione con il riciclaggio o con il finanziamento del terrorismo;
- ricevere od occultare denaro o cose provenienti da un qualsiasi delitto o compiere qualunque attività che ne agevoli l'acquisto, la ricezione o l'occultamento;
- sostituire o trasferire denaro, beni o altre utilità provenienti da illeciti, ovvero compiere in relazione ad essi altre operazioni che possano ostacolare l'identificazione della loro provenienza delittuosa;
- partecipare ad uno degli atti di cui ai punti precedenti, associarsi per commetterli, tentare di perpetrarli, aiutare, istigare o consigliare qualcuno a commetterli o agevolarne l'esecuzione.

17.4 Procedure specifiche

Ad integrazione delle procedure e regole di condotta sopra delineate, devono essere rispettate le seguenti procedure descritte per le singole aree a rischio, nonché le ulteriori procedure di volta in volta adottate da CSI.

La Banca, inoltre, già precedentemente alla realizzazione della mappatura dei Processi/Aree a rischio aveva adottato, tra le altre, specifiche procedure e global policy per la disciplina dei Processi/Aree a rischio elencati al precedente paragrafo 17.2, provvedendo al loro costante e periodico aggiornamento.

Le principali procedure/global policy a disciplina dei Processi/Aree a rischio sono elencate nell'Allegato 1 (Matrice riepilogativa procedure).

Copia digitale delle suddette procedure/policy globali è disponibile nella Intranet aziendale.

17.4.1 Gestione amministrativa clienti

La procedura di acquisizione dei clienti, di adeguata verifica, registrazione e controlli deve prevedere:

- l'adempimento degli obblighi di adeguata verifica in caso di instaurazione di un rapporto continuativo, esecuzione di operazioni occasionali (per importi pari o superiori €15.000 o in caso di operazioni "frazionate"), in presenza di sospetto di riciclaggio o finanziamento del terrorismo oppure se vi sono dubbi sulla veridicità o sull'adeguatezza dei dati già disponibili, mediante:
- l'identificazione del cliente, ottenuta sulla base di dati o informazioni provenienti da fonti affidabili ed indipendenti;
- l'identificazione dell'eventuale "titolare effettivo" e verifica dell'identità;
- la raccolta di informazioni sullo scopo e sulla natura prevista del rapporto;
- l'adozione di un approccio basato sul rischio, per cui gli obblighi di adeguata verifica della clientela si articolano in differenti gradi di *due diligence* commisurati al profilo di rischio del cliente, valutato tenendo in considerazione sia elementi soggettivi (natura giuridica, attività prevalente, comportamento del cliente al momento dell'instaurazione del rapporto o esecuzione dell'operazione, area geografica di residenza cliente o della controparte) che oggettivi (tipologia dell'operazione o del rapporto continuativo, modalità di svolgimento, ammontare dell'operazione, frequenza delle operazioni o durata del rapporto continuativo,

ragionevolezza dell'operazione/rapporto continuativo, area geografica di destinazione dell'operazione)

- la valutazione del rischio è effettuata sia in sede di instaurazione del rapporto (*ex ante*), che nel corso di tutta la durata del rapporto con il cliente (*ex post*);
- l'applicazione di obblighi di rafforzata verifica in caso di clienti non fisicamente presenti all'instaurazione del rapporto, per soggetti politicamente esposti – PEP¹³ – non residenti, per enti corrispondenti extracomunitari, per clientela con profilo di rischio riciclaggio massimo, ecc.

Nel caso di soggetti politicamente esposti (PEP), sono adottate:

- procedure specifiche per l'individuazione, la verifica, l'approvazione ed il controllo nel continuo delle Persone Politicamente Esposte;
- un iter approvativo differenziato nel caso di soggetti non-residenti o residenti, in coerenza con le disposizioni di Casa Madre;

17.4.2. Servizi bancari: gestione della liquidità, dei bonifici e dei crediti

Ad integrazione del sistema di regole e divieti precedentemente esposti, sono adottati inoltre i seguenti presidi cautelari:

- redazione di procedure dirette a definire, nel rispetto della normativa, primaria e secondaria, le modalità di attuazione degli adempimenti che integrano i presidi cautelari, assicurando l'omogeneità dei comportamenti, la loro trasparenza e la completa tracciabilità dei processi, informatici e documentali;
- identificazione dei soggetti e delle strutture responsabili della gestione dei processi con chiara attribuzione di mansioni, compiti, deleghe e responsabilità;
- *segregazione di funzioni* tra i soggetti incaricati della fase istruttoria rispetto a quelli facoltizzati alla deliberazione del finanziamento, fatte salve eventuali eccezioni stabilite dalla normativa vigente;
- adozione di sistemi informatici di supporto nella gestione delle attività di controllo per la prevenzione del riciclaggio, volti all'individuazione e selezione automatica di operazioni che presentino profili di anomalia e di rischio di riciclaggio, anche ai fini della segnalazione di operazioni sospette;
- adozione di sistemi informatici idonei ad evidenziare e bloccare l'operatività con Paesi e soggetti sottoposti a restrizioni di natura finanziaria, ovvero inclusi nelle *black list* comunitarie e/o internazionali.

17.4.3 Gestione fornitori e acquisti di beni e servizi

La procedura di **gestione fornitori, acquisto di beni e servizi** deve prevedere che:

- selezione dei fornitori e partner commerciali secondo criteri omogenei e predeterminati; tracciabilità del processo di raccolta informazioni e archiviazione;
- un adeguato processo di identificazione, approvazione e registrazione dei fornitori, consulenti e terze parti, che preveda la verifica dell'attendibilità commerciale e professionale e la verifica periodica delle correttezza ed aggiornamento delle informazioni acquisite;
- verifica della qualità di "*persone politicamente esposte*" nella controparte, ai sensi dell'art. 1 della allegato tecnico del d. lgs. 231/2007;
- verifica delle liste comunitarie ed internazionali (*black list*) in relazione all'applicazione delle sanzioni finanziarie per il contrasto del riciclaggio e del finanziamento del terrorismo;
- verifica della regolarità dei pagamenti, anche con riferimento alla coincidenza tra destinatario/ordinante e controparte effettivamente coinvolta nella transazione;

¹³ L'acronimo PEP sta per Politically Exposed Person o, in italiano, persona politicamente esposta. Per la definizione di PEP fare riferimento all'art. 1, comma 2 lettera o) del D. Lgs. n. 231/2007 e all'art. 1 dell'Allegato Tecnico al D. Lgs. n.231/2007.

Si confrontino inoltre le procedure specifiche previste per il processo “Gestione Fornitori e Acquisti” nella Parte Speciale – Reati contro la Pubblica Amministrazione.

17.4.4 Gestione del personale, degli agenti e dei promotori finanziari

Il processo di selezione del personale e dei collaboratori e degli agenti deve prevedere:

- l'adozione di procedure di selezione ed assunzione trasparenti ed omogenee, garantendo la completa tracciabilità del processo e dei criteri di selezione;
- l'esecuzione della verifica, nel pieno rispetto della normativa in materia di tutela dei dati personali, dei dati e delle informazioni raccolte in fase di selezione dai candidati;
- verifica delle liste comunitarie ed internazionali (black list) in relazione all'applicazione delle sanzioni finanziarie per il contrasto del riciclaggio e del finanziamento del terrorismo.

Si confrontino inoltre le procedure specifiche previste per il processo “Gestione del Personale” nella Parte Speciale – Reati contro la Pubblica Amministrazione.

17.4.5 Gestione delle attività di distribuzione e negoziazione con riferimento ai clienti “istituzionali”: fondi pensione (occupazionali e pre-esistenti), casse di previdenza, compagnie di assicurazione, fondazioni bancarie

Si confrontino le procedure specifiche previste per il processo “Gestione delle attività di distribuzione e negoziazione con riferimento ai clienti “istituzionali”: fondi pensione (occupazionali e pre-esistenti), casse di previdenza, compagnie di assicurazione, fondazioni bancarie” nella Parte Speciale 9 – Reati societari.

17.4.5 Gestione delle attività di sviluppo commerciale per la distribuzione di prodotti Credit Suisse nei canali Retail e Wholesales

Si confrontino le procedure specifiche previste per il processo “Gestione delle attività di sviluppo commerciale per la distribuzione di prodotti Credit Suisse nei canali Retail e Wholesales” nella Parte Speciale 9 – Reati societari.

17.4.6 Gestione delle attività di marketing per la Divisione Asset Management (selezione, negoziazione, formalizzazione, pagamento)

- è fatto divieto di stipulare contratti per l'approvvigionamento di beni o servizi nell'ambito di eventi o attività promozionali con enti, associazioni o soggetti nazionali od esteri che possano ragionevolmente essere considerati a rischio o sospetti di svolgere attività rientranti in una delle categorie di reato descritte sopra;
- è fatto divieto di riconoscere compensi in favore di fornitori esterni che non trovino adeguata giustificazione in relazione alla tipologia di incarico da svolgere ed alle prassi vigenti e che deviano da quanto concordato contrattualmente;
- nessun soggetto può da solo e liberamente accedere alle risorse finanziarie della Banca, stipulare contratti d'acquisto di beni e servizi, elargire degli omaggi, sponsorizzazioni o altra utilità, anche nel contesto della gestione di eventi e attività promozionali, senza che vi sia un altro soggetto che controlla la congruità delle operazioni e/o autorizza/approva le attività svolte e le decisioni prese;
- devono essere tracciate le transazioni effettuate e i beneficiari/soggetti invitati ad eventi e attività promozionali;
- devono essere effettuati controlli circa l'adeguatezza degli eventi e delle attività promozionali organizzati e circa la correttezza e completezza delle transazioni effettuate nell'ambito di tali eventi/attività promozionali.

Si confrontino inoltre le procedure specifiche previste per il processo “Gestione delle attività di marketing per la Divisione Asset Management (selezione, negoziazione, formalizzazione, pagamento)” nella Parte Speciale 9 – Reati societari.

17.4.7 Gestione della vendita di prodotti strutturati alla Clientela Professional

Si confrontino le procedure specifiche previste per il processo “Gestione della vendita di prodotti strutturati alla Clientela Professional” nella Parte Speciale 9 – Reati societari.

17.4.8 Gestione dei segnalatori (selezione, contrattualizzazione, pagamento)

- è fatto divieto di riconoscere compensi in favore dei segnalatori che non trovino adeguata giustificazione in relazione alla tipologia di incarico da svolgere ed alle prassi vigenti in ambito locale e che deviano da quanto concordato contrattualmente;
- è possibile procedere all'autorizzazione al pagamento dei compensi dei segnalatori solo in presenza di una verifica circa la congruità della prestazione rispetto ai termini contrattuali e di un'attenta valutazione del corrispettivo in relazione alla qualità del servizio o bene ricevuto;
- è fatto divieto di stipulare contratti di agenzia o accordi con segnalatori le cui controparti siano enti, associazioni o soggetti nazionali od osteri che possono ragionevolmente essere considerati a rischio di svolgere attività rientranti in una delle categorie di reato descritte sopra;
- nessun soggetto può, da solo e liberamente, stipulare contratti con i segnalatori, determinare o elargire le provvigioni dei segnalatori, senza che vi sia un altro soggetto che controlla la congruità delle operazioni e/o autorizza/approva le attività svolte e le decisioni prese;
- devono essere effettuati controlli circa l'adeguatezza e la corretta determinazione delle provvigioni, nonché in merito alla coerenza tra provvigione calcolata e approvata e pagamento effettuato (in termini di ammontare e controparte della transazione);
- devono essere effettuate verifiche preventive in merito alla reale esistenza, natura, affidabilità ed onorabilità dei segnalatori, anche mediante la richiesta e l'ottenimento, in fase di selezione, di idonea documentazione, attestante la presenza dei requisiti di onorabilità (quale ad esempio autodichiarazione circa l'assenza di procedimenti penali, certificato del casellario giudiziale ecc.). Tale documentazione, in caso di enti collettivi, dovrà essere riferita al legale rappresentante;
- i rapporti contrattuali con i segnalatori e le operazioni effettuate per la determinazione/controllo ed il pagamento delle provvigioni devono essere formalizzati e tracciabili.

Si confrontino le procedure specifiche previste per il processo “Gestione dei segnalatori (selezione, contrattualizzazione, pagamento)” nella Parte Speciale 9 – Reati societari.

17.4.9 Attività di origination e negoziazione dei servizi di corporate advisory

Si confrontino le procedure specifiche previste per il processo “Attività di origination e negoziazione dei servizi di corporate advisory” nella Parte Speciale 9 – Reati societari.

17.4.10 Fatturazione dei servizi di corporate advisory

- tutti gli incassi derivanti da rapporti con soggetti terzi, aumenti di capitale, incasso dividendi, ecc. sono regolati esclusivamente attraverso il canale bancario, l'unico atto ad assicurare, grazie ai moderni sistemi elettronici e telematici, adeguati livelli di sicurezza, tracciabilità ed efficienza nelle operazioni di trasferimento di denaro tra operatori economici;
- non devono essere utilizzati conti correnti o libretti di risparmio in forma anonima o con intestazione fittizia, né in Italia né presso altri Stati esteri;

- non devono essere effettuate transazioni finanziarie in denaro contante ad eccezione dei pagamenti tramite piccola cassa e comunque nel rispetto dei limiti di legge per i pagamenti in denaro contante. I pagamenti tramite piccola cassa possono avvenire solo previa verifica della documentazione giustificativa a supporto della spesa/esborso.

Si confrontino inoltre le procedure specifiche previste per il processo “Fatturazione dei servizi di corporate advisory” nella Parte Speciale 9 – Reati societari.

17.4.11 Gestione degli agenti

- è fatto divieto di riconoscere compensi in favore dei agenti che non trovino adeguata giustificazione in relazione alla tipologia di incarico da svolgere ed alle prassi vigenti in ambito locale e che deviano da quanto concordato contrattualmente;
- è possibile procedere all'autorizzazione al pagamento dei compensi degli agenti solo in presenza di una verifica circa la congruità della prestazione rispetto ai termini contrattuali e di un'attenta valutazione del corrispettivo in relazione alla qualità del servizio o bene ricevuto;
- è fatto divieto di stipulare contratti di agenzia o accordi con agenti le cui controparti siano enti, associazioni o soggetti nazionali od osteri che possono ragionevolmente essere considerati a rischio di svolgere attività rientranti in una delle categorie di reato descritte sopra;
- nessun soggetto, può da solo e liberamente stipulare contratti con gli agenti, determinare o elargire le provvigioni degli agenti, senza che vi sia un altro soggetto che controlla la congruità delle operazioni e/o autorizza/approva le attività svolte e le decisioni prese.
- devono essere effettuati controlli circa l'adeguatezza e la corretta determinazione delle provvigioni, nonché in merito alla coerenza tra provvigione calcolata e approvata e pagamento effettuato (in termini di ammontare e controparte della transazione);
- devono essere effettuate verifiche preventive in merito alla reale esistenza, natura, affidabilità ed onorabilità degli agenti, anche mediante la richiesta e l'ottenimento, in fase di selezione, di idonea documentazione, attestante la presenza dei requisiti di onorabilità (quale ad esempio autodichiarazione circa l'assenza di procedimenti penali, certificato del casellario giudiziale ecc.). Tale documentazione, in caso di enti collettivi, dovrà essere riferita al legale rappresentante;
- i rapporti contrattuali con gli agenti e le operazioni effettuate per la determinazione/controllo ed il pagamento delle provvigioni devono essere formalizzati e tracciabili.

Si confrontino inoltre le procedure specifiche previste per il processo “Gestione degli agenti” nella Parte Speciale 9 – Reati societari.

17.4.12 Gestione del sistema di remunerazione e incentivazione dei banker (dipendenti)

Si confrontino inoltre le procedure specifiche previste per il processo “Gestione del sistema di remunerazione e incentivazione dei banker (dipendenti)” nella Parte Speciale 9 – Reati societari.

17.4.13 Gestione del sistema di remunerazione e incentivazione degli agenti

Si confrontino inoltre le procedure specifiche previste per il processo “Gestione del sistema di remunerazione e incentivazione dei banker (dipendenti)” nella Parte Speciale 9 – Reati societari.

17.4.14 Amministrazione e gestione del personale (Elaborazione ed erogazioni paghe, ecc.)

- nello svolgimento del Processo a rischio in esame, CSI è supportata da un *outsourcer* esterno, al quale la Banca trasmette le informazioni necessarie all'elaborazione dei cedolini;
- la funzione HR esegue dei controlli sulle elaborazioni dei cedolini eseguite dall'*outsourcer*;

- i rapporti intercorrenti con l'outsourcer esterno che supporta la società nelle attività di cui al Processo a rischio in esame sono stati formalizzati in un apposito contratto, all'interno del quale è stata inserita una clausola 231 di presa visione e impegno al rispetto del Codice Etico e del Modello Organizzativo adottati dalla Banca;
- in caso di distacco di personale, è sempre formalizzata una lettera di distacco tra le società del gruppo interessate.

17.4.15 Gestione delle attività di marketing per la Divisione Private Banking (gestione ed organizzazione eventi, predisposizione di strumenti e materiale di comunicazione a supporto della funzione commerciale)

- è fatto divieto di stipulare contratti per l'approvvigionamento di beni o servizi nell'ambito di eventi o attività promozionali con enti, associazioni o soggetti nazionali od esteri che possano ragionevolmente essere considerati a rischio o sospetti di svolgere attività rientranti in una delle categorie di reato descritte sopra;
- è fatto divieto di riconoscere compensi in favore di fornitori esterni che non trovino adeguata giustificazione in relazione alla tipologia di incarico da svolgere ed alle prassi vigenti e che deviano da quanto concordato contrattualmente;
- nessun soggetto può da solo e liberamente accedere alle risorse finanziarie della Banca, stipulare contratti d'acquisto di beni e servizi, elargire degli omaggi, sponsorizzazioni o altra utilità, anche nel contesto della gestione di eventi e attività promozionali, senza che vi sia un altro soggetto che controlla la congruità delle operazioni e/o autorizza/approva le attività svolte e le decisioni prese;
- devono essere tracciate le transazioni effettuate e i beneficiari/soggetti invitati ad eventi e attività promozionali;
- devono essere effettuati controlli circa l'adeguatezza degli eventi e delle attività promozionali organizzati e circa la correttezza e completezza delle transazioni effettuate nell'ambito di tali eventi/attività promozionali.

Si confrontino inoltre le procedure specifiche previste per il processo "Gestione delle attività di marketing per la Divisione Divisione Private Banking (gestione ed organizzazione eventi, predisposizione di strumenti e materiale di comunicazione a supporto della funzione commerciale" nella Parte Speciale 9 – Reati societari.

14.4.16 Gestione della fiscalità (attività c.d. "new business" e consulenza);

14.4.17 Gestione della fiscalità (adempimenti fiscali)

- devono essere osservate rigorosamente tutte le disposizioni normative, anche regolamentari, a disciplina degli adempimenti di natura fiscale;
- devono essere osservate rigorosamente tutte le circolari, istruzioni e risoluzioni emanate dalle Autorità pubbliche competenti (Agenzia delle Entrate, Ministero delle Finanze, Banca d'Italia ecc.) e le procedure e global policy della Banca e di Gruppo in materia di predisposizione delle dichiarazioni fiscali e liquidazione e calcolo dei tributi;
- deve essere garantita la più ampia diffusione e conoscenza a livello aziendale delle suddette procedure e global policy;
- devono essere previste ed implementate specifiche forme di monitoraggio e controllo delle scadenze relative agli adempimenti di natura fiscale;
- i rapporti con i consulenti coinvolti nel Processo a rischio in esame devono essere debitamente formalizzati per iscritto, mediante un contratto sottoscritto secondo il sistema di poteri in essere e nel quale deve essere inserita apposita clausola di impegno al rispetto del Codice Etico e del Modello Organizzativo della Banca.

I controlli dell'Organismo di Vigilanza

L'Organismo di Vigilanza svolge controlli periodici sulle attività potenzialmente a rischio di commissione dei reati di riciclaggio, tra cui:

- verifica l'esistenza di un adeguato processo per la definizione e invio dei flussi informativi a proprio favore;
- richiede, eventualmente in via periodica, le informazioni rilevanti ai fini dell'esercizio delle proprie funzioni di vigilanza;
- verifica che l'operatività della Banca sia svolta nel rispetto della procedure interne e di Casa Madre relativamente alla prevenzione del riciclaggio e del finanziamento del terrorismo;
- verifica l'adeguatezza delle procedure di identificazione della clientela
- verifica l'adeguatezza dei presidi di prevenzione e controllo adottati in relazione alla situazione di rischio per comprendere e valutare il rischio di riciclaggio dei propri clienti;
- verifica la predisposizione dei piani formativi e la loro esecuzione ai fini di formare i dipendenti relativamente ai rischi di commissione dei reati previsti dal D.Lgs. n. 231/2007 ed ai relativi obblighi di segnalazione di operazioni sospette all'Organismo di Vigilanza;
- verifica l'adeguatezza delle procedure e delle modalità di gestione delle segnalazioni di operazioni sospette ricevute da qualsiasi fonte, interna o esterna alla Banca;

18 REATI IN MATERIA DI CRIMINALITA' ORGANIZZATA

18.1 La fattispecie di reato

L'art. 2, comma 29, della Legge n. 94 del 15 luglio 2009, "Disposizioni in materia di sicurezza pubblica", ha introdotto l'art. 24 ter del D.Lgs. n. 231/2001 "Delitti di criminalità organizzata che richiama i seguenti articoli del codice penale:

- **Associazione per delinquere finalizzata (416 c.p.)** – Associazione realizzata da tre o più persone finalizzata:
 - alla riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.);
 - alla tratta di persone (art. 601 c.p.);
 - all'acquisto e alienazione di schiavi (art. 602 c.p.);
 - ai reati concernenti le violazioni delle disposizioni in materia di immigrazione clandestina (art. 12 d. lgs. 286/1998);
- **Associazione per delinquere di stampo mafioso anche straniera (416 bis c.p.)** – Associazione di tipo mafioso formata da tre o più persone. L'associazione è di tipo mafioso quando coloro che ne fanno parte si avvalgono della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva per commettere delitti, per acquisire in modo diretto o indiretto la gestione o, comunque, il controllo di attività economiche, di concessioni, di autorizzazioni, di appalti e servizi pubblici o per realizzare profitti o vantaggi ingiusti per sé o per altri ovvero al fine di impedire od ostacolare il libero esercizio del voto o di procurare voti a sé o ad altri in occasioni di consultazioni elettorali;
- **Scambio elettorale politico mafioso (416 ter c.p.)** – Ottenimento della promessa di voti per sé o ad altri in occasione di consultazioni elettorali in cambio dell'erogazione di denaro;
- **Sequestro di persona a scopo di rapina o di estorsione (630 c.p.)** – Sequestro di una persona allo scopo di conseguire, per sé o per altri, un ingiusto profitto come prezzo della liberazione;
- **Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope** (art. 74 del d.P.R. 9 ottobre 1990, n. 309) – Associazione realizzata da tre o più persone al fine di coltivare, produrre, fabbricare, estrarre, raffinare, vendere, offrire o mettere in vendita, cedere, distribuire, commerciare, trasportare, procurare ad altri, inviare, passare o spedire in transito, consegnare per qualunque scopo sostanze stupefacenti o psicotrope;
- **Illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo** (art. 407 c.p.p.)

Con questo intervento legislativo, i delitti di criminalità organizzata diventarono presupposto di responsabilità degli enti ex D.Lgs 231/01 anche nei casi in cui tali reati non si configurino come transnazionali.

Per la società sono previste sanzioni pecuniarie da 300 a 1000 quote (da 77 migliaia di Euro a 1.549 migliaia di Euro) e sanzioni interdittive ex art. 9, comma 2 del D.Lgs. n. 231/2001, per una durata non inferiore a un anno.

18.2 Processi/Aree a Rischio

Nella tabella di sintesi sono indicate le aree individuate come sensibili alla commissione delle fattispecie di reati in materia di criminalità organizzata:

	Direzione Executive Board Collegio Sindacale	Regional Management (BPPM e ORM)	PB: Canali distribuiti	Corporate Advisory	Advisory and Sales (AOF, Product and Services, Investment Consulting)	PB: FOS Casse	CP&D	AM: Canali distribuiti	AM: Portfolio Management and Product Control	Internal Audit	Direttore Compliance	Direttore Legal	Operations	Information Technology	Credit Manager	CRES - Immobili Servizi/Sicurezza e Prevenzione	Direttore Ufficio Acquisti - Supply Mgmt	Direttore Risorse Umane	Direttore Financial Accounting
CRIMINALITA' ORGANIZZATA	Associazione per delinquere	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
	Associazione di tipo mafioso	SI	NO	SI	SI	SI	NO	NO	SI	NO	NO	NO	SI	NO	SI	NO	SI	SI	NO
	Scambio elettorale politico mafioso	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
	Sequestro di persona a scopo di rapina o di estorsione	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
	Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
	Illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO

18.3 Principi di controllo e di comportamento ed assetto del sistema di organizzazione gestione e controllo

La presente sezione illustra le regole di condotta e di comportamento nonché di assetto del sistema di organizzazione, gestione e controllo che dovranno essere seguite dai Destinatari per prevenire la costituzione di associazioni criminose all'interno della banca per la commissione di delitti legati all'attività svolta (ad esempio: reati di corruzione, reati tributari, reati societari) e di comportamenti diretti ad agevolare l'attività di associazioni criminali.

A tale scopo, devono essere adottate le seguenti regole generali:

- la scelta di *partner*, per la conclusione, sotto qualsiasi forma, di rapporti commerciali, deve avvenire nel rispetto delle procedure aziendali che devono assicurare il rispetto di criteri predeterminati e verificabili. In ogni caso, la selezione avviene preferibilmente nell'ambito di soggetti già accreditati presso la banca o la Casa Madre e comunque previa verifica della loro reputazione e affidabilità sul mercato, acquisizione e archiviazione della documentazione;
- sono chiaramente definiti ed identificati i ruoli e le responsabilità dei soggetti e delle funzioni competenti all'elaborazione dei piani di dismissione, acquisizione e sviluppo immobiliare e sono chiaramente descritte le attività assegnate a ciascuna funzione competente;
- l'acquisizione di beni o rami di azienda è effettuata solo previo svolgimento di adeguati accertamenti per verificare la legittima provenienza degli stessi;
- devono essere svolti accertamenti preventivi e commisurati al rischio per verificare la sussistenza in capo ai partner nei rapporti commerciali o al cedente di ramo d'azienda di sentenze di condanne definitive o di procedimenti penali per i reati associativi di cui all'art. 24-ter d. lgs. 231/2001, ovvero vi sia stata applicazione, o proposta di applicazione, delle misure di prevenzione, personali o patrimoniali, di cui alla l. 575/1965 e successive modifiche.

18.4 Procedure specifiche

Ad integrazione dei principi generali di comportamento, dovranno rispettarsi le regole di seguito indicate relativamente agli specifici processi:

18.4.1 Corporate Governance

Conformemente a quanto disposto dalle istruzioni di Vigilanza, sono adottati procedure e presidi che garantiscano:

- la puntuale e scrupolosa verifica dei requisiti di onorabilità e professionalità dei componenti dei vertici aziendali;
- l'adozione di una struttura di controlli adeguata a prevenire e a far emergere tempestivamente comportamenti infedeli da parte del personale della banca, nei diversi livelli di collocazione gerarchica e funzionale;
- la previsione di una struttura di controlli idonei a rilevare tempestivamente una concentrazione di responsabilità in capo a soggetti aziendali, in violazione del principio di segregazione delle funzioni.

18.4.2. Gestione ed Erogazione del credito

Nella gestione ed erogazione del credito, devono essere rispettate tutte le disposizioni previste in materia di contrasto del riciclaggio, con particolare riferimento al processo di adeguata verifica (cfr Parte Speciale 15 Reati di Riciclaggio) ed inoltre:

- deve essere previsto il divieto di porre in essere operazioni con controparti che figurino in *black list* comunitarie, internazionali o interne al gruppo di appartenenza;

- non è consentita l'erogazione di credito unicamente sulla base del "buon" nome della controparte ("name lending");
- l'erogazione del credito è consentita solo a fronte di una compiuta conoscenza della controparte, della struttura e scopo dell'operazione e della valutazione dei rischi;
- deve essere accertata l'identità dei componenti del vertice societario, la verifica di notizie negative in relazione agli stessi, la composizione del capitale ed eventuali modifiche rilevanti nella compagine societaria;
- devono essere adottate procedure, commisurate al rischio, al fine di verificare se la controparte sia stata condannata in via definitiva o sottoposta a procedimento penale per i reati associativi di cui all'art. 24-ter d. lgs. 231/2001;
- è prevista la verifica dell'adozione ed attuazione del Modello di organizzazione, gestione e controllo ex D.lgs. 231/2001 in caso di operazioni di importo significativo.

18.4.3 Gestione Fornitori e Acquisti

In aggiunta alle disposizioni previste nella Parte Speciale 8 Reati contro la Pubblica Amministrazione e 17 Reati di Riciclaggio, in particolare ove concernenti la selezione, valutazione ed approvazioni dei fornitori, sono adottate le seguenti disposizioni:

- i contratti di approvvigionamento, che possano presentare carattere inusuale o anomalo per tipologia o oggetto della richiesta, sono preventivamente valutati e autorizzati dal vertice della banca; in caso di approvazione, la conclusione dei contratti e le motivazioni a sostegno degli stessi vanno comunicati all'OdV;
- in caso di dubbio sulla qualifica o sulla permanenza della qualifica in capo al fornitore oppure in caso di sopravvenienza di profili di anomalia nei rapporti con il fornitore o nella tipologia delle richieste da questi avanzate, il rapporto può essere mantenuto solo con espressa autorizzazione del vertice della banca, previa comunicazione all'OdV;
- i Destinatari segnalano immediatamente all'OdV, oppure al proprio superiore gerarchico, che riferirà all'OdV, eventuali anomalie, di cui vengano a conoscenza, nelle prestazioni dovute dal fornitore, discordanze significative o ripetute tra materiale o servizio ricevuto rispetto a quanto concordato o particolari richieste avanzate dal fornitore alla banca;

18.5 Controlli dell'Organismo di Vigilanza

Per la descrizione dei controlli suggeriti per specifici processi, si rimanda a quanto riportato alle precedenti sezioni con riferimento a:

- Processo di Corporate Governance: Parte Speciale 8.5 Reati contro la P.A.
- Processo di Erogazione Crediti: Parte Speciale 17.5 Reati di Riciclaggio
- Processo di Gestione Fornitori e Acquisti: Parte Speciale 17.5 Reati di Riciclaggio

19 DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO

19.1 La fattispecie di reato

L'art. 25 bis.1 del D.Lgs. n. 231/2001: "Delitti contro l'industria e il commercio", richiama i seguenti articoli del codice penale:

- **Turbata libertà dell'industria o del commercio (art. 513 c.p.)** – utilizzo di violenza ovvero di mezzi fraudolenti per impedire o turbare l'esercizio di un'industria o di un commercio;
- **Illecita concorrenza con minaccia o violenza (513 bis c.p.)** – compimento di atti di concorrenza con violenza o minaccia nell'esercizio di un'attività commerciale, industriale o comunque produttiva;
- **Frodi contro le industrie nazionali (art. 514 c.p.)** – messa in vendita o altrimenti in circolazione, sui mercati nazionali o esteri, di prodotti industriali, con nomi, marchi o segni distintivi contraffatti o alterati, cagionando un nocumento all'industria nazionale;
- **Frode nell'esercizio del commercio (art. 515 c.p.)** – consegna all'acquirente di una cosa mobile per un'altra, ovvero di una cosa mobile, per origine, provenienza, qualità o quantità, diversa da quella dichiarata o pattuita nell'esercizio di una attività commerciale, ovvero in uno spaccio aperto al pubblico;
- **Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.)** – messa in vendita o altrimenti in commercio di sostanze alimentari non genuine come genuine;
- **Vendita di prodotti industriali con segni mendaci (art. 517 c.p.)** – messa in vendita o altrimenti in circolazione di opere dell'ingegno o prodotti industriali, con nomi, marchi o segni distintivi nazionali o esteri, atti a indurre in inganno il compratore sull'origine, la provenienza o la qualità dell'opera o del prodotto;
- **Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517 ter c.p.)** – fabbricazione o utilizzo industriale di oggetti o altri beni realizzati usurpando un titolo di proprietà industriale o in violazione dello stesso;
- **Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (517 quater c.p.)** – contraffazione o alterazione di indicazioni geografiche o denominazioni di origine di prodotti agroalimentari.

Per l'ente sono previste sanzioni pecuniarie fino a 800 quote (da 10 migliaia di Euro a 1.239 migliaia di Euro) e sanzioni interdittive ex art. 9, comma 2 del D.Lgs. n. 231/2001, per un periodo da tre mesi a due anni.

19.2 Processi/aree a rischio

Nel corso della verifica documentale e delle interviste con i Dirigenti e Responsabili di funzione, non sono stati rilevati profili di rischio relativamente ai reati previsti dall'art. 25 bis.1.

19.3 Principi di controllo e di comportamento ed assetto del sistema di organizzazione, gestione e controllo

La presente sezione prevede per tutti i Destinatari l'obbligo di conformarsi a tutte le politiche e procedure ed istruzioni aziendali ed in particolare al Regolamento di Direzione e prevede inoltre l'espresso divieto a carico dei responsabili di funzione, dei dipendenti e dei collaboratori esterni di

CSI di porre in essere comportamenti in grado di integrare le fattispecie di reato rientranti tra i delitti contro l'industria e il commercio.

19.5 I controlli dell'Organismo di Vigilanza

Relativamente ai reati previsti agli articoli 25.bis.1 del Decreto, non sono stati rilevati profili di rischio nel corso della fase di *assessment*, pertanto si lascia all'iniziativa dell'Odv la determinazione dei possibili controlli da svolgere a riguardo.

20 DELITTI IN VIOLAZIONE DEL DIRITTO DI AUTORE

20.1 Le fattispecie di reato

L'art. 25 novies del D.Lgs. n. 231/2001: "Delitti in materia di violazione del diritto d'autore", richiama i seguenti articoli della Legge 22 aprile 1941, n. 633:

- Immissione su sistemi di reti telematiche a disposizione del pubblico, mediante connessioni di qualsiasi genere, di opere dell'ingegno protette o parte di esse (**art. 171 comma 1**);
- Immissione su sistemi di reti telematiche a disposizione del pubblico, mediante connessioni di qualsiasi genere, di opere altrui non destinate alla pubblicazione in modo che ne risulti offeso l'onore o la reputazione dell'autore (**art. 171 comma 3**);
- Duplicazione, per trarne profitto, di programmi per elaboratore o, ai medesimi fini, importazione, distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale ovvero concessione in locazione di programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE) (**art. 171 bis**);
- Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico del contenuto di una banca di dati, ovvero estrazione, reimpiego, distribuzione, vendita o concessione in locazione di una banca dati in violazione delle disposizioni di legge (**art. 171 bis comma 2**);
- Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, di dischi, nastri o supporti analoghi ovvero di ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento (**art. 171 ter lettera comma 1 a**);
- Abusiva riproduzione, trasmissione o diffusione in pubblico, con qualsiasi procedimento, di opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati (**art. 171 ter comma 1 lettera b**);
- Introduzione nel territorio dello Stato, detenzione per la vendita o la distribuzione, o distribuzione, messa in commercio, concessione in noleggio o cessione a qualsiasi titolo, proiezione in pubblico, trasmissione a mezzo della televisione con qualsiasi procedimento, trasmissione a mezzo della radio, o riproduzione in pubblico delle duplicazioni o riproduzioni abusive di cui alle lettere a) e b) (**art. 171 ter comma 1 lettera c**);
- Detenzione per la vendita o la distribuzione, messa in commercio, vendita, noleggio, cessione a qualsiasi titolo, proiezione in pubblico, trasmissione a mezzo della radio o della televisione con qualsiasi procedimento, di videocassette, musicassette, o qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, o di altro supporto per il quale è prescritta l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (SIAE), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato (**art. 171 ter comma 1 lettera d**);
- Ritrasmissione o diffusione con qualsiasi mezzo di un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato in assenza di accordo con il legittimo distributore (**art. 171 ter comma 1 lettera e**);
- Introduzione nel territorio dello Stato, detenzione per la vendita o la distribuzione, distribuzione, vendita, concessione in noleggio, cessione a qualsiasi titolo, promozione commerciale, installazione di dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto (**art. 171 ter lettera f**);
- Fabbricazione, importazione, distribuzione, vendita, noleggio, cessione a qualsiasi titolo, pubblicizzazione per la vendita o il noleggio, o detenzione per scopi commerciali di attrezzature,

prodotti o componenti ovvero prestazione di servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure (art. **171 ter comma 1 lettera f - bis**);

- Abusiva rimozione o alterazione di informazioni elettroniche, ovvero distribuzione, importazione a fini di distribuzione, diffusione per radio o per televisione, comunicazione o messa a disposizione del pubblico di opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse (art. **171 ter comma 1 lettera h**);
- Riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o messa altrimenti in 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 (art. **171 ter comma 2 lettera a**);
- Comunicazione al pubblico attraverso immisione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o di parte di essa (art. **171 ter comma 2 lettera a - bis**);
- Esercizio in forma imprenditoriale di attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate dal diritto d'autore e da diritti connessi (art. **171 ter comma 2 lettera b**);
- Promozione o organizzazione delle attività illecite di cui al comma 1 (art. **171 ter comma 2 lettera c**);
- Mancata comunicazione alla SIAE da parte dei produttori o importatori dei supporti non soggetti al contrassegno, entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione, dei dati necessari alla univoca identificazione dei supporti medesimi (art. **171 septies lettera a**);
- Falsa dichiarazione dell'avvenuto assolvimento degli obblighi previsti dalla normativa sul diritto d'autore (art. **171 septies lettera b**);
- Produzione, messa in 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**).

Per la società sono previste sanzioni pecuniarie fino a 800 quote (da 10 migliaia di Euro a 775 migliaia di Euro) e sanzioni interdittive ex art. 9, comma 2 del D.Lgs. n. 231/2001, per un periodo da tre mesi ad un anno.

Nel corso della fase di assessment, non sono stati rilevati profili di rischio relativamente ai reati previsti dall'art. 25 novies ad esclusione dei reati previsti dall'art. 171 bis che si ritengono invece astrattamente applicabili.

20.2 Principi generali di comportamento

La presente sezione prevede per tutti i Destinatari l'obbligo di conformarsi a tutte le politiche e procedure ed istruzioni aziendali ed in particolare al Regolamento di Direzione e prevede inoltre l'espresso divieto a carico dei responsabili di funzione, dei dipendenti e dei collaboratori esterni di CSI di porre in essere comportamenti in grado di integrare le fattispecie di reato rientranti tra i delitti d'autore.

20.3 Procedure specifiche

Relativamente ai reati previsti all'art. 25 novies del Decreto, non sono stati rilevati profili di rischio nel corso della fase di *assessment* se non limitatamente ai reati di cui all'art 117 bis.

Ai fini della prevenzione di tali reati, si possono ragionevolmente ritenere applicabili ed efficaci i Principi generali di comportamento e di condotta e le Procedure Specifiche richiamate nel Capitolo 16 e già identificati come presidio della commissione dei reati di criminalità informatica, a cui si rimanda.

20.4 I controlli dell'Organismo di Vigilanza

Relativamente ai reati previsti all'art. 25 novies del Decreto, non sono stati rilevati profili di rischio nel corso della fase di *assessment*, pertanto si lascia all'iniziativa dell'Odv la determinazione dei possibili controlli da svolgere a riguardo.

21 INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA**21.1 La fattispecie di reato**

L'art. 25 novies del D.Lgs. 231/01 Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria richiama i seguenti articoli del codice penale:

- **Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377 bis c.p.)** – Reato commesso dal soggetto che, con violenza o minaccia, o con offerta o promessa di denaro o di altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere davanti l'autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, quando questa ha la facoltà di non rispondere.

In relazione alla commissione del delitto di cui all'art. 377-bis del codice penale, si applica all'ente la sanzione pecuniaria fino a cinquecento quote (da 129 mila Euro a 775 mila Euro).

21.2 Processi/Aree a rischio

Il rischio di commissione del reato è potenzialmente presente in tutte le unità organizzative.

Tuttavia, in considerazione della specificità dell'attività svolta (gestione del contenzioso, rapporti diretti con personale dipendente/collaboratori, clienti e fornitori), sono stati individuate come maggiormente sensibili al rischio le aree indicate nella tabella di sintesi:

	Direzione Executive Board Collegio Sindacale	Regional Management (BPPM e ORM)	PB: Canali distribuiti	Corporate Advisory	Advisory and Sales (AOF, Product and Services, Investment Consulting)	PB: FOS Casse	CP&D	AM: Canali distribuiti	AM: Portfolio Management and Product Control	Internal Audit	Direttore Compliance	Direttore Legal	Operations	Information Technology	Credit Manager	CRES - Immobili Servizi/Sicurezza e Prevenzione	Direttore Ufficio Acquisti - Supply Mgmt	Direttore Risorse Umane	Direttore Financial Accounting
Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	SI	NO

21.3 Principi di controllo e di comportamento ed assetto del sistema di organizzazione gestione e controllo:

E' previsto l'espresso divieto a carico dei responsabili di funzione, dei dipendenti e dei collaboratori esterni di Credit Suisse di:

- adottare comportamenti che violino i principi e le procedure aziendali previste dalla presente Parte Speciale;
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle disciplinate all'art. 377 bis del codice penale;

La presente Parte Speciale prevede, conseguentemente, l'espresso divieto a carico dei Destinatari di agire al fine di influenzare il comportamento di soggetti chiamati a rendere dichiarazioni di fronte l'autorità giudiziaria.

21.4 Procedure specifiche

Gestione del contenzioso giudiziale ed extragiudiziale

Si confrontino le procedure specifiche previste per il processo "Gestione del contenzioso giudiziale ed extragiudiziale" nella Parte Speciale – Reati contro la Pubblica Amministrazione, Par. 8.4.3, che sono qui integralmente richiamate.

I Destinatari devono inoltre:

- adottare comportamenti improntati alla massima correttezza ed etica, nel pieno rispetto dei principi sanciti dal Codice di Condotta e dalle procedure interne nei rapporti con studi legali esterni o consulenti incaricati di assistere la Banca nella gestione di contenziosi;
- operare esclusivamente nell'ambito dell'incarico ricevuto, delle deleghe e poteri conferiti e di eventuali istruzioni ricevute dall'Organismo di Vigilanza in merito all'avvio di contenzioni contrattuali, con dipendenti o attinenti l'area dei rapporti di lavoro, fiscali o di ogni altro genere;
- in relazione alle spese legali, di consulenza o inerenti accordi transattivi:
 - a. adottare adeguati processi di gestione delle risorse finanziarie;
 - b. assicurare la tracciabilità dei flussi di pagamento;
 - c. verificare le motivazioni sottostanti ad eventuali scostamenti dal budget;
- segnalare immediatamente all'Organismo di Vigilanza ogni comportamento anomalo o contrario al Codice di Condotta o alle regole e principi di comportamento stabiliti nella presente Parte Speciale.

21.5 I controlli dell'Organismo di Vigilanza

Si confrontino i controlli previsti nel corrispondente paragrafo della Parte Speciale – Reati contro la Pubblica Amministrazione, Par. 8.11 Controlli dell'Organismo di Vigilanza.

22 IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO E' IRREGOLARE**22.1 La fattispecie di reato**

L'articolo 2 del D.lgs. 16 luglio 2012, n. 109 (recante "Attuazione della direttiva 2009/52/CE che introduce norme minime relative a sanzioni e a provvedimenti nei confronti di datori di lavoro che impiegano cittadini di Paesi terzi il cui soggiorno è irregolare") ha introdotto nel Decreto l'articolo 25-*duodecies*, rubricato "Impiego di cittadini di paesi terzi il cui soggiorno è irregolare" prevedendo la responsabilità amministrativa degli enti per il reato previsto dall'art. 22, comma 12-bis del D.lgs. n. 286/1998 (Testo Unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulle condizioni dello straniero).

Di seguito si indica la fattispecie penale richiamata dall'art. 25 *duodecies* del Decreto.

Articolo 22, comma 12-bis, del decreto legislativo 25 luglio 1998, n. 286

12. Il datore di lavoro che occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno previsto dal presente articolo, ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, revocato o annullato, è punito con la reclusione da sei mesi a tre anni e con la multa di 5000,00 euro per ogni lavoratore impiegato.

12-bis. Le pene per il fatto previsto dal comma 12 sono aumentate da un terzo alla metà:

- a) se i lavoratori occupati sono in numero superiore a tre;
- b) se i lavoratori occupati sono minori in età non lavorativa;
- c) se i lavoratori occupati sono sottoposti alle altre condizioni lavorative di particolare sfruttamento di cui al terzo comma dell'articolo 603-bis del codice penale (NDR: ovvero a "situazioni di grave pericolo, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro").

22.2 Processi/Aree a rischio e Business Unit coinvolte

In considerazione della struttura e delle attività svolte la Banca, tramite l'attività di control and risk self assessment condotta (cfr. capitolo 4.2.1 "Approccio metodologico"), ha individuato il seguente Processo/Area a rischio con riferimento al reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare:

➤ *selezione del personale.*

Nella tabella di sintesi sono indicate le Business Unit a cui fanno capo la gestione e il governo del Processo/Area a rischio sopra indicato:

		Desk imprendi tori	Corporat e Advisory	PB COO	PB HEAD	Business Risk Manager	Marketin g strategic o	Products	Internal Audit	CRO Operatio nal Risk Manager	FOS / MIDDLE OFFICE	Distributi on	AM COO	Credit Risk Manage ment / Credit Consulta nt	TAX	Front Office	Business Process & Risk	HR
IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO E' IRREGOLARE	Impiego di cittadini di paesi terzi il cui soggiorno è irregolare	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	SI

22.3 Principi di controllo e di comportamento ed assetto del sistema di organizzazione, gestione e controllo

La presente sezione illustra le regole di condotta e di comportamento, nonché di assetto del sistema di organizzazione, gestione e controllo che, dovranno essere seguite dai Destinatari al fine di prevenire il verificarsi del Reato descritto al precedente Paragrafo 22.1.

La presente Parte Speciale “22” prevede l’espresso divieto – a carico dei Destinatari del presente Modello - di porre in essere comportamenti:

- tali da integrare la fattispecie di reato considerata dall’art. 25 *duodecies* del Decreto;
- che, sebbene risultino tali da non costituire di per sé la fattispecie di reato sopra considerata, possano potenzialmente diventarlo;
- non in linea o non conformi con i principi e le prescrizioni contenute nel presente Modello, nel Codice Etico e nel Codice di Condotta.
-

In particolare, i Destinatari dovranno attenersi ai seguenti principi generali di condotta:

- tenere un comportamento corretto, trasparente e collaborativo nel rispetto delle norme di legge e delle procedure interne, in tutte le attività finalizzate alla assunzione e gestione delle risorse umane;
- non intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuto o sospettato lo svolgimento di attività illecite con riferimento alle fattispecie penali punite dal “Testo Unico delle disposizioni concernenti la disciplina dell’immigrazione e norme sulle condizioni dello straniero” (di seguito “Testo Unico Immigrazione”) e, in generale, dalla normativa sulla immigrazione;
- rispettare le eventuali policy adottate dalla Banca contenenti i principi cui attenersi al fine di non violare le prescrizioni anche procedurali previste dalla normativa sull’immigrazione;
- verificare, per il tramite di pareri legali o di altri professionisti, l’eventualità che una condotta della Banca possa configurare un reato previsto dal Testo Unico Immigrazione.

22.4 Procedure Specifiche

Ad integrazione delle regole di comportamento generali, devono rispettarsi le procedure specifiche di seguito descritte per le singole aree a rischio, nonché le ulteriori procedure di volta in volta adottate da CSI.

La Banca, inoltre, già precedentemente alla realizzazione della mappatura dei Processi/Aree a rischio aveva adottato, tra le altre, specifiche procedure e global policy per la disciplina del Processo/Area a rischio elencata al precedente paragrafo 22.2, provvedendo al loro costante e periodico aggiornamento.

Le principali procedure/global policy a disciplina dei Processi/Aree a rischio sono elencate nell'Allegato 1 (Matrice riepilogativa procedure).

Copia digitale delle suddette procedure/policy globali è disponibile nella Intranet aziendale.

22.4.1 Selezione del personale

I Destinatari coinvolti nel Processo a rischio in esame devono:

- in caso di assunzione di cittadini di paesi terzi già in possesso del permesso di soggiorno, verificare l'esistenza e validità di quest'ultimo, unitamente all'ulteriore documentazione utile per perfezionare l'assunzione;
- in caso di assunzione di cittadini di paesi terzi non in possesso del permesso di soggiorno, la Banca dovrà provvedere direttamente o a mezzo del Fornitore e Consulente:
 - a) alla richiesta nominativa di nulla osta (autorizzazione all'assunzione) da presentare presso l'ufficio della Prefettura competente territorialmente;
 - b) a consegnare il nulla osta, una volta rilasciato, al cittadino che si intende assumere, affinché lo stesso possa richiedere ai competenti uffici il rilascio del visto di ingresso per motivi di lavoro subordinato e quindi, a seguito dell'ingresso in Italia, il permesso di soggiorno;
 - c) a farsi consegnare il permesso di soggiorno o la copia della domanda di rilascio del permesso di soggiorno presentata all'ufficio postale e la relativa ricevuta;
 - d) ad archiviare copia della documentazione di cui al punto c) che precede unitamente al contratto di soggiorno e lavoro;
 - e) a provvedere alle comunicazioni previste per legge al Centro per l'impiego e agli altri Enti competenti, assicurando che le informazioni trasmesse siano veritiere, complete e basate su idonea documentazione.
- mantenere monitorate le scadenze dei permessi di soggiorno e degli eventuali rinnovi dei lavoratori di paesi terzi assunti alle dipendenze/distaccati anche a mezzo dei sistemi informatici ad hoc utilizzati dalla Banca;
- inviare comunicazioni ai lavoratori di paesi terzi in prossimità della scadenza del permesso di soggiorno;
- verificare, in corso di rapporto di lavoro, la presentazione, da parte del lavoratore straniero, della domanda di rinnovo del permesso di soggiorno (di cui il lavoratore deve esibire copia della ricevuta rilasciata dall'ufficio postale presso il quale è stata effettuata la domanda), in prossimità della scadenza della validità dello stesso e comunque non oltre sessanta giorni dalla stessa;
- prevedere l'impegno del lavoratore assunto dalla Banca di trasmettere alla Banca stessa qualunque comunicazione, lettera e richiesta proveniente dalle Autorità e uffici competenti

(Questura, Prefettura, Centro per l'Impiego) in merito alla validità o scadenza del permesso di soggiorno;

- utilizzare quali intermediari per il reclutamento dei lavoratori esclusivamente Agenzie per il lavoro autorizzate dal Ministero del Lavoro, ai sensi del D.Lgs. n° 276 del 2003 (Legge Biagi);
- nei contratti con le Agenzie per il lavoro dovrà essere previsto l'inserimento di clausole con le quali:
 - a. L'agenzia si impegni espressamente a verificare l'esistenza e la validità dei permessi di soggiorno.
 - b. L'agenzia si assuma l'obbligo di monitorare le scadenze dei permessi di soggiorno e di segnalare all'utilizzatore qualsiasi controversia e contestazione proveniente dagli uffici di competenza.
 - c. L'agenzia si impegni a tenere manlevato l'utilizzatore da qualsiasi responsabilità qualora si verifichino delle irregolarità in tal senso;
- assicurare una corretta informativa e/o formazione dei Destinatari coinvolti nel Processo a rischio sopraindicato circa la normativa a disciplina dell'assunzione di lavoratori di paesi terzi;
- i contratti con i terzi coinvolti nel Processo a Rischio (Consulenti del lavoro, terzi incaricati degli adempimenti amministrativi connessi alla gestione del personale, Agenzie per il lavoro, altre Società del Gruppo ecc.) devono essere redatti secondo gli standard aziendali in uso e devono prevedere l'inserimento sistematico di una "clausola 231" in base alla quale il soggetto terzo dichiara di aver preso visione dei contenuti del Modello, del Codice Etico e del di Condotta e di impegnarsi a rispettare le prescrizioni in essi esplicitate, a pena di risoluzione del contratto;
- i Destinatari coinvolti nel Processo a rischio sono tenuti ad attenersi scrupolosamente alla documentazione organizzativa aziendale formalizzata con riferimento lo stesso;
- tutta la documentazione oggetto del presente Processo a rischio (atti, verbali, contratti, ricevute, permessi di soggiorno ed altri documenti), in formato sia elettronico che cartaceo, deve essere archiviata e facilmente rintracciabile; in particolare deve essere assicurata la tracciabilità delle fonti/elementi informativi e deve essere curata l'archiviazione di tutta la relativa documentazione prodotta/ricevuta con riferimento alle attività propedeutiche e conseguenti alla presentazione della domanda di nulla osta all'assunzione di lavoratore straniero.

22.5 I controlli dell'Organismo di Vigilanza

Si confrontino i controlli previsti nel corrispondente paragrafo della Parte Speciale – Reati contro la Pubblica Amministrazione, Par. 8.11 "I Controlli dell'Organismo di Vigilanza".

ALL. 1: Elenco delle principali procedure/global policy a disciplina dei Processi/Aree a rischio