TBWA ITALIA

Modello di organizzazione, gestione e controllo ai sensi del D. Lgs. 231/2001

PARTE SPECIALE

TBWA\ITALIA

1. RISK ASSESSMENT

1.1. Il risk assessment di TBWA

La metodologia di analisi del rischio di reato è stata messa a punto da TBWA ed estesa alle società controllate. E' un'attività che ha in primo luogo permesso di individuare e contestualizzare il rischio di reato in relazione alla governance e all'assetto organizzativo dell'ente. In secondo luogo, attraverso tale attività si è potuto ottenere informazioni utili a supportare le scelte del vertice esecutivo aziendale in merito alle azioni di adeguamento e miglioramento del modello di organizzazione, gestione e controllo dell'ente rispetto alle finalità preventive indicate dal D. Lgs. 231/2001 (quali i livelli di esposizione ai singoli rischi di reato).

L'analisi del rischio di reato è consistito, più nello specifico, nella valutazione sistematica dei seguenti fenomeni[1]:

- L'importanza di un reato (importanza)
- La frequenza con cui accade un reato (frequenza)
- L'accadimento di un reato (precedenti)

La valutazione del rischio infatti può essere espressa nella seguente formula:

Rischio di reato = F(Importanza, Frequenza, Precedenti)

In tale ottica, si riporta qui di seguito la definizione di alcuni termini fondamentali utili per comprendere la metodologia utilizzata :

- Minaccia: un'azione, un'attività, un processo o un potenziale evento nocivo caratterizzato da una frequenza di avvenimento che, in funzione della fattispecie di reato, rappresenta una possibile modalità attuativa del reato stesso.
- Vulnerabilità: mancanza di misure preventive che rende possibile l'accadimento di una minaccia e la conseguente realizzazione del reato;
- Impatto: sanzione derivante dalla realizzazione di un reato;

[1] Deve essere sottolineato che un'indagine completa circa le componenti del rischio di reato dovrebbe considerare altresì gli aspetti strettamente psicologici e personali degli apicali e dei sottoposti preposti alle attività individuate quali processi a rischio (avidità, problemi finanziari personali, scarsa lealtà verso l'organizzazione, vendetta, ecc.). Indagini di tale natura, oltre a rappresentare gravi minacce ai diritti dei lavoratori, indurrebbero l'utilizzo di informazioni aleatorie e altamente variabili (in quanto soggettive e non oggettive), nonché non permetterebbero l'assunzione di decisioni in termini di politiche correttive, in quanto facilmente sconfinanti in illeciti (con riferimento al diritto del lavoro, alla privacy, ecc.). l'analisi pertanto non ha quindi preso in considerazione tali fattori di indagine.

- Rischio di reato: è la probabilità che un determinato reato si realizzi attraverso le modalità attuative che sfruttano le vulnerabilità rappresentate dalla mancanza delle misure preventive e da un clima etico negativo.

Per analizzare il rischio di reato si è proceduto in base alle seguenti fasi operative:

- Identificazione della fattispecie di reato e conseguente individuazione delle minacce che permettono la realizzazione dei fatti di reato (in termini di condotte o attività operative)[2];

- Contestualizzazione delle minacce che permettono la realizzazione dei fatti di reato rispetto all'ente tramite tecniche di self assessment con la collaborazione attiva di avvocati e psicologi del lavoro;

- Assegnazione a ciascuna minaccia di un valore probabilistico circa il verificarsi, in base ai seguenti parametri:
  - Storia o statistica aziendale o di contesto;
  - Contesto economico e/o geografico;
  - Clima Etico e Organizzativo.

- Valutazione del livello di vulnerabilità rispetto a ciascuna minaccia, tramite l'identificazione delle misure preventive attuate;

- Valutazione dell'impatto in caso di realizzazione del rischio di reato in termini di sanzioni pecuniarie e/o interdittive.

Da un punto di vista pratico, l'analisi è stata eseguita attraverso analisi documentale e tecniche di self assessment, in modo da rilevare ed evidenziare minacce (attività a rischio di reato) non rilevabili attraverso indagini meramente documentali.

Le indagini di self assessment hanno permesso di verificare ed evidenziare la sussistenza di rischi di reato in seno alle singole aree o funzioni aziendali. L'indagine ha coinvolto i responsabili e alcuni sottoposti delle diverse aree e funzioni aziendali, i quali sono stati chiamati a rispondere alle domande con una risposta "SI/NO".

In particolare,per la capogruppo TBWA sono stati intervistati i responsabili delle seguenti Aree:

- Amministratore delegato

2 Tale fase ha avuto l'obiettivo di predefinire le cosiddette "*componenti strutturali*" del rischio di reato. L'individuazione delle componenti strutturali si è basata su una preliminare attività di interpretazione del dettato normativo (ovvero del testo della norma che prevede la sanzione penale e dei precedenti giurisprudenziali utili e necessari per una corretta interpretazione). L'attività interpretativa è stata condotta con la consulenza di primari studi legali che hanno fornito gli elementi chiave della cosiddetta fattispecie oggettiva del reato (ovvero della condotta, sia essa azione od omissione, o dell'evento previsti come punibili). Tali elementi chiave sono stati utilizzati per definire un set di domande finalizzate ad individuare le aree e le attività a rischio di reato dell'azienda costituente l'ente (tramite tecniche di self assessment). L'individuazione è resa possibile attraverso la correlazione degli elementi chiave con i dati attinenti alla realtà aziendale (organizzazione, processi, sistemi e poteri).

- Amministratori non esecutivi
- CFO
- Direttore Creativo
- Client service director
- Account director
- Responsabile IT

In caso di risposta positiva (SI), il soggetto è stato chiamato a rispondere ad un secondo set di domande, per rilevare:

- il processo o l'attività a rischio e la frequenza di pratica di tale attività,
- l'importanza di tale pratica per l'area o l'Ente e, infine,
- se è mai stato contestato un illecito in merito all'attività indicata.

Le frequenze di accadimento delle attività a rischio sono state rilevate in base a una scala di valori da 1 a 5, come evidenziato dalla seguente tabella:

RISPOSTE	DEFINIZIONI
1	Attività saltuaria
2	Attività annuale
3	Attività mensile
4	Attività settimanale
5	Attività quotidiana

Il campione aziendale sottoposto alle analisi di self assessment è stato altresì coinvolto in un'analisi del clima etico e organizzativo aziendale, finalizzata a valutare il percepito della popolazione aziendale in merito ad alcune variabili del contesto dell'ente idonee ad influenzare l'inclinazione a delinquere (spinta etica apicale, spinta etica del management, clima etico aziendale, chiarezza organizzativa e competenza del personale, politica retributiva, situazione economica e finanziaria dell'ente, adeguatezza del sistema dei controlli interni e relative capacità preventive, adeguatezza del sistema formativo, correttezza e liceità dei mercati di riferimento e approccio dell'ente ai mercati stessi, grado di accettazione del cambiamento e delle azioni preventive o correttive, adeguatezza del sistema sanzionatorio e disciplinare).

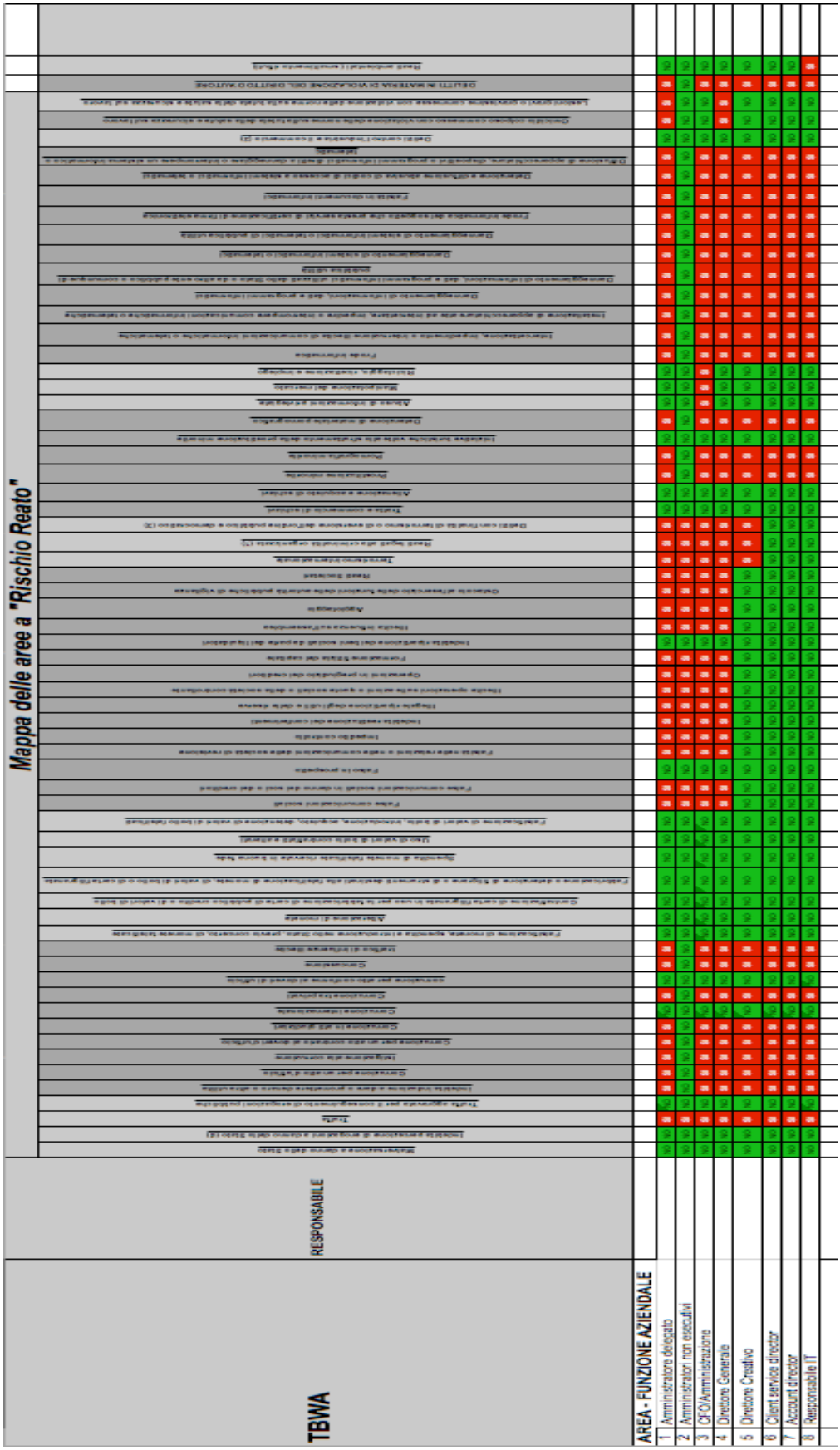
Gli intervistati hanno risposto a specifiche domande ed hanno espresso un giudizio, valorizzato utilizzando una scala di valori 1 a 5 come indicato nella seguente tabella:

RISPOSTE	DEFINIZIONI
1	negativo
2	basso

RISPOSTE	DEFINIZIONI
3	medio
4	buono
5	molto buono

I risultati dell'analisi sopra descritta sono riepilogati nella documentazione di cui alla pagina seguente: mappa delle aree a rischio.

1.2 Mappa delle aree a rischio di reato



1.3.Le aree a rischio reato ed i protocolli implementati da TBWA

Per ciascuna delle aree o funzioni aziendali che, all'esito dell'attività di indagine svolta, sono state ritenute a rischio di reato (cfr. Mappa aree a rischio), si è proceduto ad individuare i protocolli che la Società ha predisposto a presidio di ciascuno dei rischi cui la singola area è esposta.

Qui di seguito vengono quindi rappresentate le singole aree a rischio così come rappresentate nella Mappa delle aree a "Rischio Reato":

1. **Amministratore Delegato**
   - Risk Assessment 231;
   - Codice Etico;
   - Procedura sanzionatoria 231;
   - Omnicomlink/sboxportal;
   - Job description aziendale;
   - Mansionario;
   - Codice comportamentale nei rapporti con la Pubblica Amministrazione;
   - Sistema di deleghe e procure e *Grant of Authority*;
   - Procedura per la gestione dei flussi finanziari (Accounting Policies del Gruppo Omnicom e Controlli/Procedure "Sarbanes – Oxley");
   - Procedura payroll;
   - Lettera di assegnazione beni mobili (macchina-portatile-pc);
   - Procedura operativa – Erogazioni di denaro, beni o altre utilità per finalità benefico-assistenziali;
   - Accounting Policies del Gruppo Omnicom:
     - Revenue Recognition Policy
     - Retention Policy
     - Intercompany Bulletins
     - Accounting Bulletins
     - Relevant Omnicom's Memo
     - Hyperion FR Reporting Instructions;
   - Controlli/Procedure "Sarbanes-Oxley", ed in particolare:
     - Key Control Sox - Test
     - Key Control Sox - Financial Reporting
     - Key Control Sox – Control Environment;
     - Key Control Sox – Account Payable
     - Key Control Sox – Account Receivable
     - Key Control Sox – Payroll
   - Procedura internazionale per la gestione di omaggi e regalie;
   - Sistema di salute e sicurezza aziendale;
   - Procedura privacy e per la gestione e utilizzo dei sistemi informativi aziendali – green book.
   - Codice comportamentale anticorruzione

2. Amministratori non esecutivi

- Risk Assessment 231;
- Codice Etico;
- Procedura sanzionatoria 231;
- Omnicomlink/sboxportal;
- Job description aziendale;
- Mansionario;
- Codice comportamentale nei rapporti con la Pubblica Amministrazione;
- Sistema di deleghe e procure e *Grant of Authority*;
- Accounting Policies del Gruppo Omnicom:
  - Revenue Recognition Policy
  - Retention Policy
  - Intercompany Bulletins
  - Accounting Bulletins
  - Relevant Omnicom's Memo
  - Hyperion FR Reporting Instructions;
- Controlli/Procedure "Sarbanes-Oxley", ed in particolare:
  - Key Control Sox - Test
  - Key Control Sox - Financial Reporting
  - Key Control Sox – Control Environment;
  - Key Control Sox – Account Payable
  - Key Control Sox – Account Receivable
  - Key Control Sox – Payroll
- Lettera di assegnazione beni mobili (macchina-portatile-pc);
- Procedura operativa – Erogazioni di denaro, beni o altre utilità per finalità benefico –assistenziali;
- Procedura payroll;
- Procedura internazionale per la gestione di omaggi e regalie;
- Procedura per la gestione dei flussi finanziari (Accounting Policies del Gruppo Omnicom e Controlli/Procedure "Sarbanes – Oxley").
- Codice comportamentale anticorruzione

3. CFO

- Risk Assessment 231;
- Codice Etico;
- Procedura sanzionatoria 231;
- Omnicomlink/sboxportal;
- Job description aziendale;
- Mansionario;
- Codice comportamentale nei rapporti con la Pubblica Amministrazione;
- Sistema di deleghe e procure e *Grant of Authority*;
- Procedura per la gestione dei flussi finanziari (Accounting Policies del Gruppo Omnicom e Controlli/Procedure "Sarbanes-Oxley");

- Procedura payroll;
- Lettera di assegnazione beni mobili (macchina-portatile-pc);
- Procedura operativa – Erogazioni di denaro, beni o altre utilità per finalità benefico-assistenziali;
- Accounting Policies del Gruppo Omnicom:
  - Revenue Recognition Policy
  - Retention Policy
  - Intercompany Bulletins
  - Accounting Bulletins
  - Relevant Omnicom's Memo
  - Hyperion FR Reporting Instructions;
- Controlli/Procedure "Sarbanes-Oxley", ed in particolare:
  - Key Control Sox - Test
  - Key Control Sox - Financial Reporting
  - Key Control Sox – Control Environment;
  - Key Control Sox – Account Payable
  - Key Control Sox – Account Receivable
  - Key Control Sox – Payroll;
- Procedura privacy e oer la gestione e l'utilizzo dei sistemi informativi aziendali – green book;
- Procedura internazionale per la gestione di omaggi e regalie.
- Codice comportamentale anticorruzione

5. Direttore Creativo

- Risk Assessment 231;
- Codice Etico;
- Procedura sanzionatoria 231;
- Omnicomlink/sboxportal;
- Job description aziendale;
- Mansionario;
- Codice comportamentale nei rapporti con la Pubblica Amministrazione;
- Sistema di deleghe e procure e *Grant of Authority*;
- Procedura per la gestione dei flussi finanziari (Accounting Policies del Gruppo Omnicom e Controlli/Procedure "Sarbanes-Oxley");
- Procedura payroll;
- Lettera di assegnazione beni mobili (macchina-portatile-pc);
- Procedura operativa – Erogazioni di denaro, beni o altre utilità per finalità benefico-assistenziali;
- Procedura internazionale per la gestione di omaggi e regalie;
- Procedura privacy e per la gestione e utilizzo dei sistemi informativi aziendali.
- Codice comportamentale anticorruzione

6. **Client Service director**
   - Risk Assessment 231;
   - Codice Etico;
   - Procedura sanzionatoria 231;
   - Omnicomlink/sboxportal;
   - Job description aziendale;
   - Mansionario;
   - Codice comportamentale nei rapporti con la Pubblica Amministrazione;
   - Sistema di deleghe e procure e *Grant of Authority*;
   - Procedura per la gestione dei flussi finanziari (Accounting Policies del Gruppo Omnicom e Controlli/Procedure "Sarbanes-Oxley");
   - Procedura payroll;
   - Lettera di assegnazione beni mobili (macchina-portatile-pc);
   - Procedura operativa – Erogazioni di denaro, beni o altre utilità per finalità benefico-assistenziali;
   - Procedura privacy e per la gestione e utilizzo dei sistemi informativi aziendali.
   - Codice comportamentale anticorruzione

7. **Account director**
   - Risk Assessment 231;
   - Codice Etico;
   - Procedura sanzionatoria 231;
   - Omnicomlink/sboxportal;
   - Job description aziendale;
   - Mansionario;
   - Codice comportamentale nei rapporti con la Pubblica Amministrazione;
   - Sistema di deleghe e procure e *Grant of Authority*;
   - Procedura per la gestione dei flussi finanziari (Accounting Policies del Gruppo Omnicom e Controlli/Procedure "Sarbanes-Oxley");
   - Procedura payroll;
   - Lettera di assegnazione beni mobili (macchina-portatile-pc);
   - Procedura operativa – Erogazioni di denaro, beni o altre utilità per finalità benefico-assistenziali;
   - Procedura privacy e per la gestione e utilizzo dei sistemi informativi aziendali.
   - Codice comportamentale anticorruzione

2. PIANO DI GESTIONE DEL RISCHIO

Sulla base degli esiti del risk Assessment è stato possibile elaborare il "Piano di gestione del rischio", che ha identificato i protocolli preventivi già esistenti o da elaborare per l'abbattimento del rischio di reato ad una misura accettabile (da intendersi nella residuale "*possibilità di commettere un illecito solo violando dolosamente un protocollo preventivo*").

Il piano è rappresentato da una tabella, qui di seguito riprodotta, in cui sono indicate le seguenti informazioni:

- i rischi di reato da prevenire (ovvero i singoli Reati da prevenire, per classi di reato);

- i protocolli preventivi per l'abbattimento del rischio di reato al livello ritenuto accettabile dall'Ente, suddivisi in protocolli generici per tutti i tipi di reato e protocolli specifici per determinate classi di reato);

- lo stato di attuazione dei protocolli (Attuato/In Attuazione) e l'esistenza delle procedure operative.

Le procedure operative già formalizzate dalla Società, sono state valutate in ottica 231 per verificare la loro efficacia come protocolli preventivi in relazione ai correlati Reati presuppost

1. Protocolli generici

Tutti i Reati	1 Analisi del rischio di reato		
	1.1 Identificazione dei rischi di reato	A	Risk Assessment 231
	• Mappatura Aree a rischio	A	Risk Assessment 231
	• Individuazione modalità attuative	A	Risk Assessment 231
	1.2 Valutazione dei livelli di rischio di reato, clima etico e aziendale e soggettivo	A	Risk Assessment 231
	• Analisi impatti	A	Risk Assessment 231
	• Analisi protocolli preventivi	A	Risk Assessment 231
	2 Protocolli inerenti la formazione e l'attuazione delle decisioni		
	2.1 Corporate Governance	A	Sistema deleghe e procure
	• Analisi responsabilità e funzioni	A	Sistema deleghe e procure, Organigramma
	• Formalizzazione poteri (autorizzativi, firma e spesa) con limiti adeguati alle responsabilità delle funzioni	A	Sistema deleghe e procure
	• Firma congiunta	A	Sistema deleghe e procure
	• Contrapposizione di funzioni	A	Sistema deleghe e procure
	• Revisione	A	Sistema deleghe e procure
	2.2 Formalizzazione processi	A	
	• Analisi processi aziendali	A	Omnicomlink/sboxportal
	• Formalizzazione dei processi aziendali	A	Omnicomlink/sboxportal
	• Sistema informativo aziendale	A	Omnicomlink/sboxportal
	• Separazione delle funzioni	A	Omnicomlink/sboxportal
	• Attività di formazione	A	Job description aziendale – profilo della funzione
	• Revisione	N	Gestito a livello internazionale
	2.3 Procedure operative	A	
	• Formalizzazione PO Ciclo attivo	A	Omnicomlink/sboxportal
	Formalizzazione PO gare d'appalto	A	
	• Formalizzazione PO Ciclo passivo	A	Omnicomlink/sboxportal
	• Formalizzazione PO Contabilità	A	Omnicomlink/sboxportal
	• Formalizzazione PO HR	A	Omnicomlink/sboxportal
	• Formalizzazione PO utilizzo beni e risorse finanziarie	A	Omnicomlink/sboxportal
	• Formalizzazione PO informazione specifica	A	
	• Attività di comunicazione e sensibilizzazione	A	
	• Attività di formazione	A	
	2.4 Job description per le principali funzioni	A	Mansionario/Job Description aziendale
	• Formalizzazione job description	A	Mansionario/Job Description aziendale
	• Attività di comunicazione e sensibilizzazione	A	Mansionario/Job Description aziendale

Tutti i Reati	• Attività di formazione	A	Mansionario/Job Description aziendale
	• Revisione	A	Mansionario/Job Description aziendale
	3 Protocolli di controllo		
	3.1 Istituzione dell'organismo di controllo ex d. lgs. 231/2001	A	Regolamento dell'organismo di vigilanza 231 e piano di audit annuale
	• Controlli di efficacia ex ante	A	Regolamento dell'organismo di vigilanza 231 e piano di audit annuale
	• Controlli di legalità	A	Regolamento dell'organismo di vigilanza 231 e piano di audit annuale
	• Controlli di effettività del modello	A	Regolamento dell'organismo di vigilanza 231 e piano di audit annuale
	• Reporting e segnalazioni	A	Regolamento dell'organismo di vigilanza 231 e piano di audit annuale
	• Sistemi di segnalazione anonima	A	Regolamento dell'organismo di vigilanza 231 e piano di audit annuale
	3.2 Funzione internal audit	A	Accounting Policies del Gruppo Omnicom e Controlli/Procedure "Sarbanes Oaxley"
	• Controlli di efficacia ex ante	A	Accounting Policies del Gruppo Omnicom e Controlli/Procedure "Sarbanes Oaxley"
	• Controlli di legalità	A	Accounting Policies del Gruppo Omnicom e Controlli/Procedure "Sarbanes Oaxley"
	• Controlli di effettività del modello	A	Accounting Policies del Gruppo Omnicom e Controlli/Procedure "Sarbanes Oaxley"
	• Reporting e segnalazioni	A	Accounting Policies del Gruppo Omnicom e Controlli/Procedure "Sarbanes Oaxley"
	3.3 Sistema dei controlli interni	A	Accounting Policies del Gruppo Omnicom e Controlli/Procedure "Sarbanes Oaxley"
	• Pianificazione dei controlli	A	Accounting Policies del Gruppo Omnicom e Controlli/Procedure "Sarbanes Oaxley"
	• PO per i controlli interni	A	Accounting Policies del Gruppo Omnicom e Controlli/Procedure "Sarbanes Oaxley"
	• Reporting e segnalazioni	A	Accounting Policies del Gruppo Omnicom e Controlli/Procedure "Sarbanes Oaxley"
	3.4 Controllo di gestione	A	Accounting Policies del Gruppo Omnicom e Controlli/Procedure "Sarbanes Oaxley"
	• Controlli con efficacia preventiva (Black list, controlli tempi, modi e luoghi pagamento, blocchi autorizzativi, ecc)	A	Accounting Policies del Gruppo Omnicom e Controlli/Procedure "Sarbanes Oaxley"
	• Controllo di gestione ex post	A	Accounting Policies del Gruppo Omnicom e Controlli/Procedure "Sarbanes Oaxley"
	4 Adozione di Standard		
	UNI-INAIL	A	Sistema salute sicurezza sul lavoro
	5 Codice etico		
	5.1 Formalizzazione del codice etico	A	Codice Etico (che comprende il Code of Business Conduct del Gruppo Omnicom)
	5.2 Previsione di norme di condotta riferite ai Reati	A	Codice Etico (che comprende il Code of Business Conduct del Gruppo Omnicom)
	5.3 Conformità requisiti minimi associazioni di categoria	A	Codice Etico (che comprende il Code of Business Conduct del Gruppo Omnicom)
	5.4 Comunicazione e sensibilizzazione	A	Codice Etico (che comprende il Code of Business Conduct del Gruppo Omnicom)
	5.5 Formazione	A	Codice Etico (che comprende il Code of Business Conduct del Gruppo Omnicom)

Tutti i Reati	5.6 Revisione	A	Codice Etico (che comprende il Code of Business Conduct del Gruppo Omnicom)
	6 Apparato sanzionatorio e disciplinare		
	6.1 Apicali	A	Procedura sanzionatoria 231
	6.2 Personale dipendente sottoposto	A	Procedura sanzionatoria 231
	6.3 Fornitori o terzi che operano per conto dell'ente o che intrattengono rapporti con la società	A	Procedura sanzionatoria 231

2.Protocolli specifici

REATO		PROTOCOLLO
REATI INERENTI FINANZIAMENTI PUBBLICI, TRUFFE E FRODI AI DANNI DELLO STATO O DI ALTRI ENTI PUBBLICI	A	Codice comportamentale nei rapporti con la Pubblica Amministrazione
	A	Sistema di deleghe e procure e *Grant of Authority*
DELITTI DI CRIMINALITA' ORGANIZZATA	A	Procedura per la gestione dei flussi finanziari (Accounting Policies del Gruppo Omnicom e Controlli/Procedure "Sarbanes-Oxley)
	A	Sistema di deleghe e procure e *Grant of Authority*
	A	Lettera di assegnazione beni mobili (macchina-portatile-pc) Circolare per l'utilizzo dei beni aziendali
	A	Procedura payroll (Accounting Policies del Gruppo Omnicom e Controlli/Procedure "Sarbanes-Oxley)
	A	Procedura internazionale per la gestione di omaggi e regalie
REATI SOCIETARI	A	Accounting Policies del Gruppo Omnicom: ➢ Revenue Recognition Policy ➢ Retention Policy ➢ Intercompany Bulletins ➢ Accounting Bulletins ➢ Relevant Omnicom's Memo ➢ Hyperion FR Reporting Instructions Controlli/Procedure "Sarbanes-Oxley", ed in particolare: ➢ Key Control Sox - Test ➢ Key Control Sox - Financial Reporting ➢ Key Control Sox – Control Environment; ➢ Key Control Sox – Account Payable ➢ Key Control Sox – Account Receivable ➢ Key Control Sox – Payroll
REATI IN MATERIA DI IGIENE SICUREZZA SUL LAVORO	A	Sistema di salute e sicurezza sul lavoro aziendale
RICETTAZIONE, RICICLAGGIO, IMPIEGO DI DENARO, BENI O UTILITA' DI PROVENIENZA ILLECITA	A	Procedura per la selezione e gestione dei fornitori
	A	Procedura per la gestione dei flussi finanziari (Accounting Policies del Gruppo Omnicom e Controlli/Procedure "Sarbanes-Oxley)
ARTT. 317 - 322 BIS C.P. - TUTTI I REATI CORRUTTIVI E CONCUSSIONE - UTILITÀ DI SCAMBIO	A	Procedura per la gestione delle spese di rappresentanza (in attuazione)
	A	Procedura per la gestione dei flussi finanziari (Accounting Policies del Gruppo Omnicom e Controlli/Procedure "Sarbanes-Oxley)
	A	Procedura per la selezione e gestione dei fornitori
	A	Procedura payroll
	A	Lettera di assegnazione beni mobili (macchina-portatile-pc)
	A	Procedura operativa - Erogazioni di denaro, beni o altre utilità per finalità benefico-assistenziali
	A	Sistema di deleghe e procure e Grant of Authority
	A A	Codice comportamentale nei rapporti con la Pubblica Amministrazione Codice comportamentale anticorruzione

REATO		PROTOCOLLO
DELITTI CON FINALITÀ DI TERRORISMO O DI EVERSIONE DELL'ORDINE DEMOCRATICO ART. 270-BIS C.P. ASSOCIAZIONI CON FINALITÀ DI TERRORISMO ANCHE INTERNAZIONALE O DI EVERSIONE DELL'ORDINE DEMOCRATICO	A	Procedura per la selezione e gestione dei fornitori
	A	Lettera di assegnazione beni mobili (macchina-portatile-pc)
	A	Procedura operativa - Erogazioni di denaro, beni o altre utilità per finalità benefico-assistenziali
	A	Sistema di deleghe e procure e Grant of Authority
	A	Procedura per la gestione dei flussi finanziari (Accounting Policies del Gruppo Omnicom e Controlli/Procedure "Sarbanes-Oxley)
	A	Procedura payroll
	A	Lettera di assegnazione beni mobili (macchina-portatile-pc)
REATI INFORMATICI	A	Procedura privacy e per la gestione e utilizzo dei sistemi informativi aziendali - green book
DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE	A	Procedura per la gestione del diritto d'autore
INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITA' GIUDIZIARIA	A	Codice comportamentale nei rapporti con la Pubblica Amministrazione

1. Sistema Informatico Gestionale "AS 400" (N.B. è attualmente in corso la migrazione verso il sistema "MAP");
2. Circolari Periodiche TBWA;
3. *Green Book* TBWA;
4. *Blue Book* TBWA;
5. *Grant of Authority* del Gruppo Omnicom;

6. Specifiche Procedure adottate ai sensi del Decreto:

   - *Codice comportamentale nei rapporti con la Pubblica Amministrazione;*
   - *Procedura erogazioni;*
   - *Procedura clausole contrattuali;*
   - *Procedura Interessi degli Amministratori;*
   - *Codice Comportamentale Anticorruzione*

3. PIANO DI ATTIVITÀ

La Società ha terminato l'elaborazione dei protocolli preventivi prima indicati come "in attuazione", come previsto nel Piano di Attività e di Audit e di attività redatto dall'Organismo di Controllo.

Si intende ora procedere :

- alla messa a punto di **nuove modalità per i Flussi Informativi dalle funzioni all'Organismo di Controllo di TBWA e per i flussi informativi dagli Organismi di Controllo delle società partecipate all'Organismo di Controllo di TBWA**

Allegati alla Parte Speciale

1. Codice Etico

2. Sistema disciplinare

3. Regolamento dell'Organismo di Controllo

4. Flussi Informativi dalle funzioni all'Organismo di Controllo **(T.B.Revised)**

5. Procedure organizzative 231
   - *Codice comportamentale nei rapporti con la Pubblica Amministrazione;*
   - *Procedura erogazioni;*
   - *Procedura clausole contrattuali;*
   - *Procedura Interessi degli Amministratori*
   - *Codice Comportamentale Anticorruzione*