MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D. LGS. N. 231/2001

B: PARTE SPECIALE

Edizione 1 – Revisione 7

Documento approvato dal Consiglio di Amministrazione di ETJCA S.p.A.

Gestione del Documento

☐ Copia CONTROLLATA N.

Questo Documento è distribuito in copia controllata, registrata e soggetta ad aggiornamento.

Destinatario: _____

☐ Copia NON CONTROLLATA

Questo Documento, distribuito in copia non controllata, ha carattere unicamente informativo e non è soggetta ad aggiornamento.

Revisioni della Prima Edizione del Documento			
N° REV.	*DATA*	*OGGETTO*	*PARAGRAFO/ I*
1	28/06/2011	Emissione ufficiale del documento.	tutti
2	31/03/2013	Introduzione del Reato di favoreggiamento all'immigrazione clandestina e valutazione del rischio.	Par. 13
		Modifiche dei tempi di attuazione dei programmi preventivi.	tutti
		Sostituzione temine "Riesame della Direzione" con Piano Annuale e Relazione Finale.	tutti
3	08/06/2016	Modificata valutazione reati contro la Pubblica Amministrazione.	Par. 1
		Modificata valutazione reati societari.	Par. 2
		Modificata valutazione reati informatici.	Par. 4
		Modificata valutazione reati riconducibili a inosservanza norme sulla sicurezza.	Par. 5
		Modificata valutazione reati di Ricettazione, Riciclaggio e Autoriciclaggio.	Par. 10
		Modificata valutazione reati di Ricettazione, Riciclaggio e Autoriciclaggio.	Par. 13
4	16/01/2020	Aggiornato capitolo relativo ai Rapporti con la Pubblica Amministrazione relativamente al D.Lgs. N. 50/2016 (c.d. Codice degli Appalti).	Cap. 1
		Aggiornato capitolo e misure di prevenzione reti riconducibili a situazioni classificabili come corruzione di dipendenti della P.A.	Cap. 1
		Aggiornamento delle procedure di controllo derivanti dall'utilizzo di fonti di finanziamento pubblico nell'ambito della formazione finanziata.	Cap. 1
		Valutazione di commissione di reati dei reati di corruzione tra privati.	Cap. 14
		Valutazione di commissione di reati dei reati di razzismo e xenofobia.	Cap. 15
		Valutazione di commissione di reati di tipo tributario e modalità di controllo.	Cap. 16
		Valutazione di commissione di reati di frode in competizioni sportive ed esercizio abusivo di gioco o scommesse e giochi d'azzardo.	Cap. 17
5	30/03/2021	Inserimento modifiche di cui al D.Lgs. N. 75/2020: frode in pubbliche forniture, frode nei reati di indebita compensazione, omessa dichiarazione e dichiarazione infedele.	Capp. 1.4, 16
		Inserimento modifiche di cui al D.Lgs. N. 75/2020: reato di contrabbando.	Cap. 18
		precisazioni sul tema della partecipazione agli appalti pubblici	Cap. 1
		Precisazioni in merito alla procedura da adottare nel caso di richieste relative al certificato del Casellario Giudiziale per lavoratori che rientrano nel dettato del D.Lgs. N. 74/2016.	Cap. 4.4
6	24/02/2022	Introdotto D.Lgs. 8 novembre 2021, n. 184, che recepisce la Direttiva Europea 2019/713 "relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti".	Cap. 9
		Introdotto D.Lgs. 8 novembre 2021, n. 195, in attuazione della Direttiva Europea 2018/1673 "sulla lotta al riciclaggio mediante il diritto penale".	Cap. 10
7	10/01/2023	Aggiornamento normativo sul tema di market abuse, introduzione reato di frodi in edilizia e danni contro il patrimonio culturale, Aggiornamento normativo sul tema degli attacchi contro Sistemi Informativi, implementazione dei controlli in materia di prevenzione di frodi fiscali	Capp. 1, 4, 6, 7, 16,
Verificato da O.d.V.:		Approvato dal C.d.A.:	

Indice dei Contenuti

PREMESSA

PARTE B: PARTE SPECIALE

CAPITOLO 1: Reati commessi contro la Pubblica Amministrazione

1.1 – Principali riferimenti normativi
1.2 – Analisi iniziale
1.3 – Valutazione del Rischio
1.4 – Misure e Procedure

CAPITOLO 2: Reati Societari

2.1 – Principali riferimenti normativi
2.2 – Analisi iniziale
2.3 – Valutazione del Rischio
2.4 – Misure e Procedure

CAPITOLO 3: Reati di Abuso di Mercato

3.1 – Principali riferimenti normativi
3.2 – Analisi iniziale
3.3 – Valutazione del Rischio
3.4 – Misure e Procedure

CAPITOLO 4: Reati Informatici e reati contro la *privacy*

4.1 – Principali riferimenti normativi
4.2 – Analisi iniziale
4.3 – Valutazione del Rischio
4.4 – Misure e Procedure

CAPITOLO 5: Reati derivanti dall'inosservanza di norme sulla sicurezza e la tutela della salute dei lavoratori

5.1 – Principali riferimenti normativi
5.2 – Analisi iniziale
5.3 – Valutazione del Rischio
5.4 – Misure e Procedure

CAPITOLO 6: Reati da violazione del diritto d'autore

6.1 – Principali riferimenti normativi
6.2 – Analisi iniziale
6.3 – Valutazione del Rischio
6.4 – Misure e Procedure

CAPITOLO 7: Reati contro la personalità individuale

7.1 – Principali riferimenti normativi
7.2 – Analisi iniziale
7.3 – Valutazione del Rischio
7.4 – Misure e Procedure

CAPITOLO 8: Reati contro l'Industria e Il Commercio

8.1 – Principali riferimenti normativi
8.2 – Analisi iniziale
8.3 – Valutazione del Rischio
8.4 – Misure e Procedure

CAPITOLO 9: Falsità in monete, carte di credito, valori di bollo

9.1 – Principali riferimenti normativi
9.2 – Analisi iniziale
9.3 – Valutazione del Rischio
9.4 – Misure e Procedure

CAPITOLO 10: Reati di Ricettazione, Riciclaggio e Autoriciclaggio

10.1 – Principali riferimenti normativi
10.2 – Analisi iniziale
10.3 – Valutazione del Rischio
10.4 – Misure e Procedure

CAPITOLO 11: Reati in materia ambientale

11.1 – Principali riferimenti normativi
11.2 – Analisi iniziale
11.3 – Valutazione del Rischio
11.4 – Misure e Procedure

CAPITOLO 12: Criminalità organizzata, terrorismo, eversione, reati transnazionali

12.1 – Principali riferimenti normativi
12.2 – Analisi iniziale
12.3 – Valutazione del Rischio
12.4 – Misure e Procedure

CAPITOLO 13: Reato di corruzione tra privati

13.1 – Principali riferimenti normativi
13.2 – Analisi iniziale
13.3 – Valutazione del Rischio
13.4 – Misure e Procedure

CAPITOLO 14: Reato di favoreggiamento dell'immigrazione clandestina e utilizzo di manodopera irregolare

14.1 – Principali riferimenti normativi
14.2 – Analisi iniziale
14.3 – Valutazione del Rischio
14.4 – Misure e Procedure

CAPITOLO 15: Reati di razzismo e xenofobia

15.1 – Principali riferimenti normativi
15.2 – Analisi iniziale
15.3 – Valutazione del Rischio
15.4 – Misure e Procedure

CAPITOLO 16: Reati di tipo tributario

16.1 – Principali riferimenti normativi
16.2 – Analisi iniziale
16.3 – Valutazione del Rischio
16.4 – Misure e Procedure

CAPITOLO 17: Frode in competizioni sportive ed esercizio abusivo di gioco o scommesse e giochi d'azzardo

17.1 – Principali riferimenti normativi
17.2 – Analisi iniziale
17.3 – Valutazione del Rischio
17.4 – Misure e Procedure

CAPITOLO 18: Reato di Contrabbando

17.1 – Principali riferimenti normativi
17.2 – Analisi iniziale
17.3 – Valutazione del Rischio
17.4 – Misure e Procedure

PREMESSA

La Parte Speciale B del Modello ha lo scopo di illustrare il Sistema di prevenzione e controllo nel suo complesso adottato ai sensi del Decreto Legislativo 8 giugno 2001 n. 231.

Il documento Parte Speciale B del Modello è suddiviso in Capitoli in riferimento alle singole fattispecie di reato richiamate dal D.Lgs. 231/01 (o similari fattispecie di reato) in modo che risulti possibile effettuare una prima valutazione strutturata preliminare ed eventualmente escludere talune fattispecie di reato che non prevedono fattori di rischio rilevanti.

Attraverso una fase diagnostica basata su analisi dei processi, interviste opportunamente documentate, documenti esaminati, ecc., è stato possibile individuare, per singola fattispecie di reato, attività "sensibili" nell'ambito delle quali è teoricamente possibile una commissione del reato.

Qualora, a seguito della valutazione del rischio, una determinata fattispecie di reato costituisca elemento d'attenzione, nel capitolo corrispondente viene descritto il Sistema di prevenzione e controllo adottato deputato alla prevenzione dei reati nell'ambito delle attività sensibili elencate. Il Sistema dei controlli si fonda su prassi operative e su Documenti del Sistema formalmente approvati, diffusi e applicati in ETJCA S.p.A. Il Sistema di prevenzione prevede la redazione di Procedure e Protocolli. Le Procedure sono state redatte per la gestione, fase dopo fase, di un processo particolarmente complesso e potenzialmente rischioso. I Protocolli viceversa sono assimilabili a istruzioni operative in quanto tendono a specificare dettagliatamente fasi o micro-fasi di un determinato processo già di per sé pianificato in documenti o non rischioso nel complesso di tutte le fasi del processo ma soltanto in alcune di esse.

I documenti del Sistema rappresentano quindi l'attuazione dei principi generali di comportamento che sono stati compiutamente definiti nel Codice Etico, che qui s'intende integralmente richiamato, nonché un insieme di regole e strumenti di controllo, volti alla prevenzione dei reati rilevanti nell'ambito delle attività sensibili che trovano attuazione nelle procedure operative.

Ai fini della predisposizione del presente Modello e alla luce dell'analisi dei seguenti aspetti:

- attività svolte;
- contesto socioeconomico in cui la Società opera;
- rapporti e relazioni giuridiche ed economiche che la Società instaura con soggetti terzi;
- colloqui con i vertici aziendali e interviste svolte con i responsabili di funzione.

ETJCA S.p.A. si impegna a valutare costantemente la rilevanza ai fini del presente Modello di eventuali ulteriori reati previsti attualmente dal Decreto o nelle sue successive integrazioni.

L'Organismo di Vigilanza vigila affinché le procedure operative diano piena attuazione ai principi e alle prescrizioni contenute nei successivi Capitoli. I Protocolli e le Procedure operative sono costantemente aggiornati anche su proposta dell'Organismo di Vigilanza al fine di garantire il raggiungimento delle finalità del Modello.

PARTE B: PARTE SPECIALE

CAPITOLO 1: Reati commessi contro la Pubblica Amministrazione

1.1 – Principali riferimenti normativi

Articoli di Legge	Cod.
art. 316 bis c.p., malversazione a danno dello Stato;	1.1
art. 316 ter c.p., indebita percezione di erogazioni a danno dello Stato;	1.2
art. 640 c. 2 c.p., Truffa in danno dello Stato o di un ente pubblico;	1.3
art. 640 bis c.p., Truffa aggravata per il conseguimento di erogazioni pubbliche;	1.4
art. 640 ter c.p., Frode informatica in danno dello Stato o di altro ente pubblico	1.5
art. 317 c.p. Concussione;	1.6
art. 318 c.p. Corruzione per un atto d'ufficio;	1.7
art. 319 c.p. Corruzione per un atto contrario ai doveri d'ufficio;	1.8
Art. 319 c.p. ter, Corruzione in atti giudiziari	1.9
art. 320 c.p. Corruzione di persona incaricata di un pubblico servizio;	1.10
art. 322 c.p. Istigazione alla corruzione;	1.11
art. 322 bis c.p. Peculato, concussione, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri;	1.12
Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria ex art. 25-novies, D.Lgs. 231/01; articolo aggiunto dalla L. 3 agosto 2009 n. 116, art. 4 (art. 377-bis c.p.);	1.13
Legge 6 novembre 2012, n. 190 recante "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella Pubblica Amministrazione";	1.14
D.Lgs. 50/2016 (c.d. Codice degli Appalti);	1.15
Regolamento (UE) N. 1303/2013 del Parlamento Europeo e del Consiglio del 17 dicembre 2013 recante disposizioni comuni sul Fondo Europeo di Sviluppo Regionale, sul Fondo Sociale Europeo, sul Fondo di Coesione, sul Fondo Europeo Agricolo per lo Sviluppo Rurale e sul Fondo Europeo per gli Affari Marittimi e la Pesca e disposizioni generali sul Fondo Europeo di Sviluppo Regionale, sul Fondo di Coesione e sul Fondo Europeo per gli Affari Marittimi e Pesca.	1.16
D.Lgs. N. 75/2020: introduzione del reato di frode in pubbliche forniture	1.17

1.2 – Analisi iniziale

La seguente matrice identifica le aree (funzioni e processi) oggetto di indagine in riferimento ai rischi specifici.

Funzioni/Aree	Processi, fasi e attività	N. casistica
C.d.A.	Linee di indirizzo economico e finanziario	1, 2
Amministrazione	Gestione dei rapporti e dei flussi finanziari in entrata (gestione degli incassi) e in uscita intrattenuti con soggetti terzi. Gestione delle vendite beni ed alienazione cespiti	1, 2
Risorse Umane	Gestione dei rapporti contrattuali con i dipendenti di struttura e somministrati e gestione dei progetti	1
Approvvigionamenti	Gestione degli approvvigionamenti di beni e servizi	1
Area Clienti/Filiali	Rapporti con i Clienti	1
Politiche Attive	Erogazione e rendicontazione progetti e servizi al lavoro finanziati	1, 2
Divisione Formazione	Erogazione e rendicontazione di progetti finanziati di formazione professionale	1, 2
Divisione Gare per la PA	Processo di partecipazione a Gare pubbliche	3

Processi				Giudizio Preliminare [2]	Controlli Esistenti						Valutazione Controlli [3]	Ruolo della Funzione					
Sigla Area/Funz.	N. Fase/Attività	Cod. Reato	Fattore [1]		Esistenza di Procedure	Aggiornamento Procedure	Esistenza di Deleghe	Conoscenza e Comunicazione	Suddivisione Compiti	Controlli e Monitoraggi		Operativo	Decisionale	Autorizzativo	Monitoraggio	Sanzionatorio	*Training*
C.d.A.	1,2	1	I, E, D	M	☒	☒	☑	☑	☑	☑	M	☑	☑	☑	☑	☑	☒
AMM	1,2	1	I, E, D	M	☒	☒	☑	☑	☑	☑	M	☑	☑	☑	☑	☒	☒
RU	1	1	I, E, D	B	☑	☑	☑	☑	☑	☑	E	☑	☑	☒	☑	☒	☒
CLI	1	1	I, E, D	M	☑	☑	☑	☑	☑	☑	M	☑	☑	☒	☑	☒	☒
ACQ	1	1	I, E, D	B	☑	☑	☑	☑	☑	☑	E	☑	☑	☒	☑	☒	☒
AM	1, 2	1	I, E	M	☑	☑	☑	☑	☑	☑	E	☑	☑	☒	☑	☒	☑
PAL	1, 2	1	I, E	M	☑	☑	☑	☑	☑	☑	E	☑	☑	☒	☑	☒	☑
DF	1, 2	1	I, E	M	☑	☑	☑	☑	☑	☑	E	☑	☑	☒	☑	☒	☑
DGare	3	1	I, E	M	☑	☑	☑	☑	☑	☑	E	☑	☑	☒	☑	☒	☑

1 I = Interno, E = Esterno, D = Decisionale. **2** Giudizio preliminare rischio reato: A = Alto, M = Medio, B = Basso, I = Inesistente. **3** Valutazione efficacia e adeguatezza dei controlli: I = Inefficaci, M = da migliorare, E = Efficaci, N = Non Esistenti. 4 ☒ = Elemento non presente; ☑ = Elemento Presente.

Il D.Lgs. 231/01 individua, fra le diverse fattispecie, le ipotesi corruttive, nelle varie forme, di malversazione ai danni dello stato e di indebita percezione di erogazioni pubbliche, cui si aggiungono la truffa ai danni dello stato e la frode informatica, di cui agli artt. art. 640, II comma, n. 1, 640 bis e 640 ter c.p. Il soggetto passivo del reato è la Pubblica Amministrazione, secondo l'accezione estesa individuata dalla giurisprudenza.

Elemento essenziale nei reati contro la PA è la distinzione tra "funzione pubblica" e "pubblico servizio".

Per **funzione pubblica** si intende l'esercizio delle attività, disciplinate da norme di Diritto Pubblico, attinenti alla funzione legislativa, amministrativa e giudiziaria. La funzione pubblica è caratterizzata dall'esercizio del potere autoritativo e del potere certificativo. Colui che "esercita una pubblica funzione legislativa, giudiziaria o amministrativa" è qualificato, ai sensi dell'art. 357 c.p., "Pubblico Ufficiale".

Per **pubblico servizio** si intende, invece, l'esercizio delle attività di produzione di beni e servizi di interesse generale e assoggettate alla vigilanza di un'Autorità Pubblica o l'esercizio delle attività volte a garantire i diritti fondamentali della persona, quali quello alla vita, alla salute, alla libertà, alla previdenza e assistenza sociale, all'istruzione, alla libertà di comunicazione ecc. Il pubblico servizio è un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri autoritativi e certificativi. Colui che "a qualunque titolo presta un pubblico servizio" è qualificato, ai sensi dell'art. 358 c.p., "persona incaricata di un pubblico servizio".

A titolo esemplificativo, ma non esaustivo, nell'ambito delle attività della Società i soggetti con cui si instaurano rapporti "sensibili" sono pubblici ufficiali/incaricati di pubblico servizio: i funzionari ministeriali o delle amministrazioni locali, gli incaricati dalla PA (di funzione pubblica o pubblico servizio) per l'effettuazione di visite di accreditamento, monitoraggi e rendicontazioni, i funzionari dell'ASL, ecc.

Alla luce del processo di adozione del Modello, in particolare delle attività di *risk assessment* svolte, sono state ritenute significative o potenzialmente tali ai fini dell'attuazione del Decreto, le seguenti attività sensibili:

1. la gestione di procedure di gara o di negoziazione diretta per l'assegnazione di commesse (servizi, progetti);
2. la partecipazione a procedure di gara o di negoziazione diretta indette da Enti Pubblici per l'assegnazione di commesse, di concessioni o altre operazioni similari caratterizzate comunque dal fatto di essere svolte in un contesto potenzialmente competitivo, intendendosi tale anche un contesto in cui, pur essendoci un solo concorrente in una particolare procedura, l'ente appaltante avrebbe avuto la possibilità di scegliere anche altre imprese presenti sul mercato;
3. la partecipazione a procedure per l'ottenimento di erogazioni, contributi o finanziamenti da parte di organismi pubblici italiani o comunitari ed il loro concreto impiego;
4. la partecipazione a procedure per l'ottenimento da parte della PA di provvedimenti autorizzativi rilevanti;
5. l'intrattenimento di rapporti con esponenti della PA che abbiano competenze in processi legislativi, regolamentari, di controllo o amministrativi/autorizzativi riguardanti le attività svolte, quando tali rapporti possano comportare l'ottenimento di vantaggi rilevanti per la Società, dovendosi escludere l'attività di mera informativa, partecipazione a eventi o momenti istituzionali e scambio di opinioni relativamente a particolari politiche o normative.
6. l'assunzione di personale (compresa la selezione e la somministrazione).

Il D.lg. 25 febbraio 2022, n. 13 avente ad oggetto "Misure urgenti per il contrasto alle frodi e per la sicurezza nei luoghi di lavoro in materia edilizia, nonché sull'elettricità prodotta da impianti da fonti rinnovabili", è intervenuto apportando modifiche ad una serie di reati contro la pubblica amministrazione, tutti inseriti nell'alveo dei reati presupposto del D.Lgs. 231/2001. Nello specifico, il Legislatore:

- ha modificato il titolo di reato dell'articolo 316-bis c.p., ora rubricato "Malversazione di erogazione pubblica" anziché "Malversazione ai danni dello Stato"
- ha ampliato l'operatività delle fattispecie di indebita percezione di erogazioni pubbliche ex art. 316-ter c.p. e di truffa aggravata per il conseguimento di erogazioni pubbliche ex art. 640-bis al fine di includere nelle suddette fattispecie anche le frodi inerenti al bonus fiscale 110%.
- ha previsto l'introduzione della fattispecie contro il patrimonio culturale anche nel catalogo dei reati presupposto ex D.Lgs. 231/2001, con la previsione di sanzioni fino a 900 quote e l'applicabilità sanzioni interdittive per una durata massima di due anni.

Relativamente all'ampliamento delle fattispecie di reato riconducibili a malversazione o a frodi in materia edilizia (es. finanziamenti 110% per ristrutturazioni) e danni contro il patrimonio culturale, allo stato attuale non sono previste casistiche rilevanti e rischi potenziali.

1.3 – Valutazione del Rischio

Annotazioni Casistica 1

Tenuto conto della rilevanza attribuita dal D.Lgs. 231/2001, ETJCA S.p.A. ritiene di includere anche soggetti che, sebbene presentino formalmente una natura privatistica, sono contraddistinti dal carattere pubblicistico dell'attività esercitata ovvero dalla rilevante presenza di partecipazioni da parte di soggetti pubblici (figure che assumono rilevanza al fine della commissione di tali tipologie di reati sono quelle dei pubblici ufficiali e degli incaricati di pubblico servizio).

Per i reati riconducibili a casi di corruzione o di istigazione alla corruzione, ETJCA S.p.A. ha continuativi rapporti con soggetti della PA. L'ordinaria gestione delle proprie attività di *business* è caratterizzata da numerose fattispecie di controlli, tra esse troviamo:

- controlli esercitati nell'ambito della regolarità dei rapporti di lavoro di soggetti somministrati o dipendenti direttamente assunti da ETJCA S.p.A. (es. Ispettorato del Lavoro, INAIL, INPS, ecc.);
- controlli di primo, secondo e terzo livello condotti da parte di enti di controllo istituzionali o incaricati di pubblico servizio (es. Unione Europea, Regione, Città Metropolitana, Controlli di Enti privati, ecc.);
- verifiche di rendicontazione attività e progetti (consuntivo economico finanziamento);
- ispezioni per il mantenimento dell'Accreditamento regionale condotto da Funzionari regionali o soggetti incaricati;
- Ispezioni condotte dall'Agenzia per le entrate e da Funzionari e da rappresentanti della GDF in ordine alla situazione tributaria;
- Ispezioni riconducibili alla corretta gestione del Sistema di Igiene del Lavoro e di prevenzione infortuni sul lavoro.

Sempre in questa fattispecie rientrano quelle attività legate ai rapporti che si possono intrattenere con i soggetti incaricati delle valutazioni dei progetti finalizzati alla concessione o meno di un finanziamento pubblico.

La situazione riconducibile a queste tipologie di controlli di per sé pur non presentando un'incidenza statistica di rischio elevata in quanto nel passato non si sono verificati casi acclarati o presunti di corruttela, tuttavia non è possibile classificarla come irrilevante in quanto non possono escludersi aprioristicamente situazioni ascrivibili a casi di corruzione, soprattutto i termini di godimento di prestazioni e favori.

Modalità e contesti di commissione del reato: Casistica 1

Per i reati riconducibili a casi di corruzione, di istigazione alla corruzione, concussione, ecc. le modalità in cui potrebbero verificarsi casi sono circoscritti ai numerosi rapporti interpersonali come scritto al § precedente. In particolare, potrebbero generarsi potenziali situazioni in cui, con lo scopo di eludere ispezioni o ottenere vantaggi nei controlli o vantaggi nelle attribuzioni di progetti o, ancora, autorizzazioni, si promettano, o si accetti di conferire (concussione), somme in denaro, situazioni lavorative per i familiari, regalie, favori, ecc.

Rischi e ricadute Casistica 1

Per i reati riconducibili a casi di corruzione/concussione, più che per motivi di probabilità di accadimento, i rischi sono elevati soprattutto in termini di gravità e incidenza del fattore di rischio. Una situazione, seppure incidentale e occasionale, potrebbe genare problematiche non soltanto di rilevanza penale per chi ha commesso il fatto, ma, oltre

alle conseguenze previste dal D.Lgs. 231/01, potrebbero generarsi anche situazioni potenzialmente pericolose sia per il mantenimento dello stato di accreditamento, sia per l'immagine che ETJCA S.p.A. si è costruita nel corso degli anni.

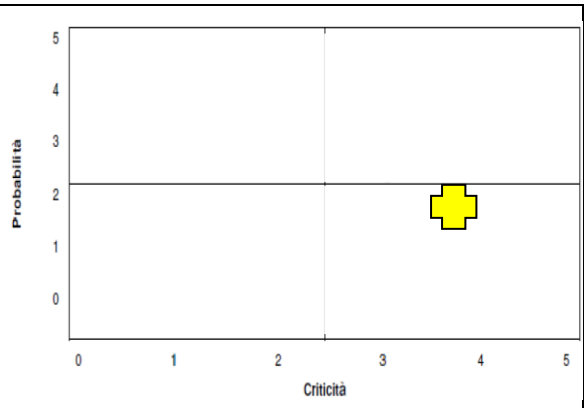
Controlli esistenti Casistica 1

Esiste una formale ripartizione di compiti, responsabilità e autorità. In particolare, in caso di sopralluogo, monitoraggio, ispezione, ecc. è previsto che interagiscano con i soggetti controllori i diretti responsabili delle funzioni che, a loro volta, si interfacciano e relazionano direttamente con la Direzione in caso di controlli e ne riferiscono immediatamente gli esiti. Esistono inoltre controlli nell'ambito delle assunzioni di personale interno.

Quantificazione Casistica 1

Nell'ambito dei singoli rischi di reato, potenzialmente attivi in specifiche aree aziendali, se ne valuta la *magnitudo* sulla base delle variabili: probabilità e impatto e, in relazione al valore ottenuto e agli scostamenti, si definisce un piano operativo definendo le tipologie di misure preventive e di controllo da attuare.

Probabilità							
Molto alta	0,45	0,00	2,25	4,50	9,00	18,00	36,00
Alta	0,35	0,00	1,75	3,50	7,00	14,00	28,00
Media	0,25	0,00	1,25	2,50	5,00	10,00	20,00
Bassa	0,15	0,00	0,75	1,50	3,00	6,00	12,00
Molto bassa	0,05	0,00	0,25	0,50	1,00	2,00	4,00
Nulla	0,00	0,00	0,00	0,00	0,00	0,00	0,00
		0	5	10	20	40	80
		Nullo	Molto basso	Basso	Medio	Alto	Molto alto
		Impatto					



Probabilità	Impatto	Indice di Valutazione:
0,15	**40**	**6**

La Magnitudo si ottiene moltiplicando le variabili P e I (**M = P * I**); da cui ne deriva che l'Esposizione che può essere classificata **Bassa**, **Media** o **Elevata**. Strategie di *risk response*. Per un rischio alto: **evitare** il rischio (*risk avoidance*), per un rischio medio: **limitare** il rischio (*risk reduction*) o **trasferire** il rischio (*risk transferring/sharing*), per il rischio basso: **accettare** il rischio (*risk acceptance*).

Annotazioni Casistica 2

Per i reati di: frode, indebita percezione, malversazione, ecc. si possono delineare situazioni rilevanti più da un punto di vista procedura e operativo più che da fatti/atti dolosi; tuttavia, la seconda accezione non è da escludere in quanto, sebbene improbabile, le ricadute potrebbero essere rilevanti e pericolose.

In particolare, si rileva un potenziale rischio nella corretta gestione dei flussi di cassa (ciclo attivo e ciclo passivo) in ordine alla riferibilità delle spese dirette e indirette come previsto dai vigenti Regolamenti europei per il FSE o similari e pericoli di commissione dei reati di indebita percezione e malversazione (tuttavia poco probabili in quanto i flussi di cassa sono tenuti costantemente sotto controllo e con conti bancari separati rispetto alle attività a libero mercato).

Si rileva un potenziale rischio di cattiva gestione della documentazione che attesta la regolare erogazione di un servizio/progetto, ecc.

Inoltre, si rileva un potenziale rischio in termini di affidabilità Economica e Finanziaria (requisito essenziale per chi eroga azioni finanziate in ambito FSE o legate a fondi interprofessionali).

Al momento non si segnalano situazioni di rischio di frode informatica in quanto i sw messi a disposizione dagli Enti Finanziatori, e le procedure esistenti che prevedono un'adeguata suddivisione di compiti e responsabilità, garantiscono sufficientemente la nostra Organizzazione.

Modalità e contesti di commissione del reato: Casistica 2

Potrebbero verificarsi casi di:

- irregolarità di tipo economico e finanziario nel caso in cui mancassero requisiti di rintracciabilità e riferibilità dei flussi economici relativi ai singoli progetti (ex Regolamento UE N. 1303/2013);

- erronea registrazione dei costi diretti del personale attribuito alla singola attività o progetto (es. errata consuntivazione di attività svolte da personale interno mediante *time-sheet*) tale da generare scarsa riferibilità al progetto specifico rispetto al monte ore di lavoro per individuo;
- erronea attribuzione di incarichi a professionisti e conseguente erronea registrazione di fatture passive;
- erronea registrazione del costo diretto dovuto all'approvvigionamento di materiale (bene di consumo, attrezzature apparecchiatura HW o SW);
- carenza nella tenuta dei documenti comprovanti le attività erogate (registri);
- potenziali problematiche nella gestione della documentazione attestante la regolare iscrizione di Utenti (es. iscrizioni di utenti che non hanno titolo);
- erogazione di corsi differenti rispetto ai progetti presentati e approvati dagli Enti Finanziatori, ecc.;
- irregolarità riconducibili alla produzione di documentazione contrattuale all'atto della presentazione di progetti, di contratti con le imprese nell'ambito di corsi in conto formazione, azioni di consulenza per il lavoro ecc.

Rischi e ricadute Casistica 2

Potrebbero generarsi rischi di decurtazioni finanziamenti e di sanzioni derivanti la mancata gestione di processi (Accreditamenti Regionali) con conseguenti ricadute sulla situazione di cassa, penalizzazioni, riscontri negativi sugli stati di Accreditamento e, *extrema ratio*, rischi di aperture di fascicoli di rilevanza penale o amministrativa.

Controlli esistenti Casistica 2

Esiste una formale ripartizione di compiti, responsabilità e autorità. In particolare, esiste una procedura volta al controllo dei singoli progetti finanziati, dalla fase di programmazione, fino all'erogazione, consuntivazione e rendicontazione economica. La procedura contiene fasi di programmazione generale, monitoraggi di corsi e attività, controllo dei corsi erogati e relativi esiti e controlli preliminari alla rendicontazione. Le Sedi trasmettono i programmi formativi alla Sede centrale, la Sede centrale monitora le fasi di erogazione del corso attraverso un sistema di controlli documentali (*random*) e sopralluoghi e, alla fine del corso, richiede i registri.

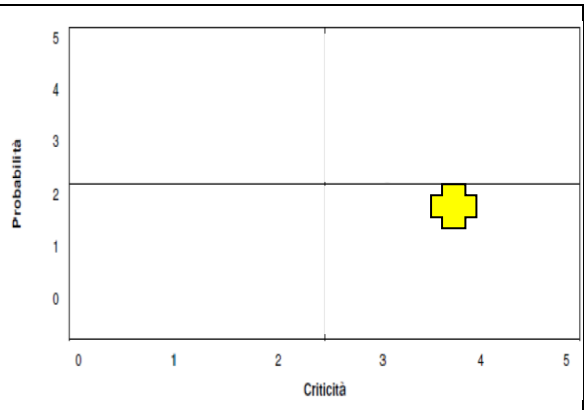
I documenti contabili vengono registrati direttamente sul sw gestionale ed esiste inoltre un controllo finale preliminare alla rendicontazione. Da un punto di vista economico il flusso prevede l'emissione di una richiesta interna del dirigente, l'emissione dell'ordine con visione del AMM, ricevimento fattura, ricerca dell'ordine (uff. fornitori), registrazione e pagamento da parte della tesoreria (autorizzato da AMM via bancaria).

Infine, esistono flussi di cassa controllati in quanto è aperto uno specifico Conto Corrente a garanzia del requisito di tracciabilità dei flussi economici in entrata da Enti Pubblici (a norma dell'art. 3, comma 7 della legge 13/08/2010 n. 136, come successivamente modificato dal D.L. 187 del 12/11/2010 e infine convertito in legge n. 217 del 17/12/2010). Per questo conto corrente sono attive formali deleghe a operare. Inoltre, i flussi di cassa sono tenuti sotto controllo dagli organi collegiali della Società.

Quantificazione Casistica 2

Nell'ambito dei singoli rischi di reato, potenzialmente attivi in specifiche aree aziendali, se ne valuta la *magnitudo* sulla base delle variabili: probabilità e impatto e, in relazione al valore ottenuto e agli scostamenti, si definisce un piano operativo definendo le tipologie di misure preventive e di controllo da attuare.

Probabilità							
Molto alta	0,45	0,00	2,25	4,50	9,00	18,00	36,00
Alta	0,35	0,00	1,75	3,50	7,00	14,00	28,00
Media	0,25	0,00	1,25	2,50	5,00	10,00	20,00
Bassa	0,15	0,00	0,75	1,50	3,00	6,00	12,00
Molto bassa	0,05	0,00	0,25	0,50	1,00	2,00	4,00
Nulla	0,00	0,00	0,00	0,00	0,00	0,00	0,00
		0	5	10	20	40	80
		Nullo	Molto basso	Basso	Medio	Alto	Molto alto
		Impatto					



Probabilità	Impatto	Indice di Valutazione:
0,15	**40**	**6**

La Magnitudo si ottiene moltiplicando le variabili P e I (**M = P * I**); da cui ne deriva che l'Esposizione che può essere classificata **Bassa**, **Media** o **Elevata**. Strategie di *risk response*. Per un rischio alto: **evitare** il rischio (*risk avoidance*), per un rischio medio: **limitare** il rischio (*risk reduction*) o **trasferire** il rischio (*risk transferring/sharing*), per il rischio basso: **accettare** il rischio (*risk acceptance*).

Annotazioni Casistica 3

Il terzo caso si riferisce alla partecipazione alle gare di appalto per i contratti di somministrazione stipulati con soggetti della Pubblica Amministrazione; si ritengono maggiormente a rischio i casi di affidamento diretto da parte della Stazione Appaltante nell'ambito dei quali potrebbero verificarsi casi di tentativi di corruzione.

Modalità e contesti di commissione del reato: Casistica 3

Le attività di licitazione e gare ad affidamento diretto potrebbero dare luogo a elementi di commistione e non improbabili rapporti di eccessivo vicinato tra Stazione Appaltante e rappresentante di Etjca.

Rischi e ricadute Casistica 3

Potrebbero verificarsi situazioni rischiose in termini di illeciti nella partecipazione a gare di appalto o anche soltanto richieste di chiarimento da parte dell'autorità competente ANAC.

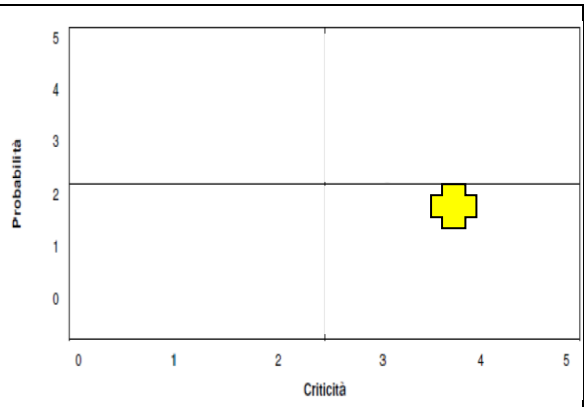
Controlli esistenti Casistica 3 (rinvio alla Procedura del Sistema Qualità PRO Gare)

Esiste una formale ripartizione di compiti, responsabilità e autorità. Per le modalità operative vedere la Procedura del Sistema Qualità PRO Gare.

Quantificazione Casistica 3

Nell'ambito dei singoli rischi di reato, potenzialmente attivi in specifiche aree aziendali, se ne valuta la *magnitudo* sulla base delle variabili: probabilità e impatto e, in relazione al valore ottenuto e agli scostamenti, si definisce un piano operativo definendo le tipologie di misure preventive e di controllo da attuare.

Probabilità							
Molto alta	0,45	0,00	2,25	4,50	9,00	18,00	36,00
Alta	0,35	0,00	1,75	3,50	7,00	14,00	28,00
Media	0,25	0,00	1,25	2,50	5,00	10,00	20,00
Bassa	0,15	0,00	0,75	1,50	3,00	6,00	12,00
Molto bassa	0,05	0,00	0,25	0,50	1,00	2,00	4,00
Nulla	0,00	0,00	0,00	0,00	0,00	0,00	0,00
		0	5	10	20	40	80
		Nullo	Molto basso	Basso	Medio	Alto	Molto alto
		Impatto					



Probabilità	Impatto	Indice di Valutazione:
0,15	**40**	**6**

La Magnitudo si ottiene moltiplicando le variabili P e I (**M = P * I**); da cui ne deriva che l'Esposizione che può essere classificata **Bassa**, **Media** o **Elevata**. Strategie di *risk response*. Per un rischio alto: **evitare** il rischio (*risk avoidance*), per un rischio medio: **limitare** il rischio (*risk reduction*) o **trasferire** il rischio (*risk transferring/sharing*), per il rischio basso: **accettare** il rischio (*risk acceptance*).

1.4 – Misure e Procedure

In considerazione della magnitudo del rischio con livello di esposizione medio ma con, tuttavia, un alto impatto in termini di ricadute e pericolosità, si ritiene opportuno integrare l'attuale sistema dei controlli e delle deleghe con azioni specifiche di controllo e presidio poste in essere a cura e sotto il controllo dell'O.d.V..

Le procedure preventive dovranno essere attivate al fine di:

- osservare strettamente tutte le leggi e regolamenti che disciplinano l'attività aziendale, con particolare riferimento alle attività che comportano contatti e rapporti con la Pubblica Amministrazione ed alle attività relative allo svolgimento di una pubblica funzione o di un pubblico servizio;
- instaurare e mantenere qualsiasi rapporto con la Pubblica Amministrazione sulla base di criteri di massima correttezza e trasparenza, in considerazione dell'imparzialità che deve ispirare l'attività amministrativa;
- controllare con cura tutti i flussi di cassa riferibili a finanziamenti pubblici e garantirne la loro tracciabilità in riferimento allo specifico progetto.

Quali misure preventive è fatto espresso divieto per i Destinatari di:

- attuare comportamenti tali da integrare le fattispecie di reato sopra considerate;
- realizzare qualsiasi situazione anche solo di rischio potenziale in relazione a quanto previsto dalle suddette ipotesi di reato.

- attuare comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;

In particolare, è fatto espresso divieto di:

- effettuare elargizioni in denaro a pubblici ufficiali o incaricati di pubblico servizio;
- promettere o elargire favori o servigi di qualsiasi tipo tali da indurre l'adozione di un comportamento omissivo da parte del dipendente della PA o dell'incaricato di pubblico sevizio;
- effettuare promesse di assunzioni dirette o di prossimi congiunti fino al terzo grado che possano apparire come finalizzati allo scambio di favori con soggetti pubblici o incaricati di pubblico servizio;
- distribuire omaggi e regali al di fuori di quanto previsto dalla prassi aziendale, vale a dire, ogni forma di regalo eccedente le normali pratiche commerciali o di cortesia o comunque rivolta ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale. In particolare, è vietata qualsiasi forma di regalo a funzionari pubblici, o a loro familiari, che possa influenzarne la discrezionalità o l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per la società. Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore, o perché volti a promuovere l'immagine della società;
- riconoscere compensi in favore dei Collaboratori esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alle prassi vigenti in ambito locale;
- effettuare prestazioni in favore dei *partner* che non trovino adeguata giustificazione nel contesto del rapporto associativo costituito con i *partner* stessi;
- ricevere o sollecitare elargizioni in denaro, omaggi, regali, o vantaggi di altra natura, nell'ambito dell'esercizio di pubbliche funzioni o di pubblico servizio, ove eccedano le normali pratiche commerciali e di cortesia;

Ai fini dell'attuazione dei comportamenti di cui sopra l'O.d.V. vigilerà affinché:

- di ciascuna operazione a rischio venga conservato un adeguato supporto documentale che consenta di procedere in ogni momento a controlli in merito alle caratteristiche dell'operazione, al relativo processo decisionale, alle autorizzazioni rilasciate per la stessa e alle verifiche su di essa effettuate;
- ETJCA S.p.A. non inizi o prosegua alcun rapporto con Destinatari del presente Modello che non intendono allinearsi al principio della stretta osservanza delle leggi e dei regolamenti vigenti;
- gli incarichi conferiti ai Collaboratori esterni siano redatti per iscritto, con l'indicazione del compenso pattuito e devono essere proposti, verificati o approvati da almeno due soggetti appartenenti a ETJCA S.p.A. che ne abbiano il potere;
- che i flussi finanziari siano tenuti sotto controllo mediante tracciabilità delle spese dirette e indirette (riferimento al codice progetto nella causale) e che confluiscano in specifico conto bancario;
- nessun tipo di pagamento venga effettuato in contanti o in natura, tranne che per circostanze eccezionali dovute a comprovata necessità;
- coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività (pagamento di fatture, destinazione di finanziamenti ottenuti dallo Stato o da organismi comunitari, ecc.) pongano attenzione all'attuazione degli adempimenti stessi da parte dei soggetti incaricati.
- le dichiarazioni rese a soggetti pubblici per l'ottenimento di erogazioni, contributi o finanziamenti, contengano solo informazioni veritiere e, in caso di ottenimento delle relative somme, venga redatto apposito rendiconto;

Casistica 1

Per quanto attiene alle assunzioni di personale è, come si è detto, vietato effettuare promesse di assunzioni dirette o di prossimi congiunti fino al terzo grado che possano apparire come finalizzati allo scambio di favori con soggetti pubblici o incaricati di pubblico servizio. In questo caso non esiste il divieto assoluto di assumere, per esempio, un parente di un dipendente dalla PA, sarà tuttavia necessario valutare caso per caso allo scopo di individuare eventuali potenziali relazioni di causa ed effetto (per es prometto di assumere un parente di un incaricato dell'Ispettorato del Lavoro cui compete controllare una ns. sede territoriale). A questo scopo è necessario che il soggetto che è in procinto di essere assunto firma apposta dichiarazione che attesta l'assenza di un conflitto di interessi in questo senso (con, inoltre, un impegno futuro a informare Etjca su eventuali nuove situazioni).

Sul tema dei rapporti interpersonali con soggetti della PA, è comunque importante rimarcare la suddivisione di compiti e responsabilità esistenti e modalità operative su Protocollo di Sistema (confermando continuativi flussi informativi interfunzionali e verso l'O.d.V.). In linea di principio per tutte le operazioni nell'ambito delle attività sensibili deve sempre essere individuato un Responsabile Interno che, salvo diversa indicazione, si identifica con il Responsabile della funzione competente per la gestione dell'operazione considerata.

Successivamente, anche in questo caso, è necessario condividere principi e modalità operative mediante formazione interna e mediante la distribuzione di Codice Etico e Regime Sanzionatorio.

Anche in questo caso l'O.d.V., come prevede sia la Parte Generale A, sia il proprio Regolamento, consuntiva annualmente lo stato dell'arte e dispone aggiornamenti nella valutazione di questa fattispecie di commissione reato. L'O.d.V., come prevede sia la Parte Generale A, sia il proprio Regolamento, riassume annualmente lo stato dell'arte e dispone aggiornamenti nella valutazione di questa fattispecie di commissione reato.

Infine, considerando la Legge 6 novembre 2012, n. 190 recante "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella Pubblica Amministrazione", sarebbe opportuno che l'O.d.V. acquisisca le necessarie informazioni relative alla figura apicale (Dirigente Responsabile), in seno a un determinato Ufficio della P.A., nominato quale referente per l'applicazione della suddetta legge e, nel caso di problematiche/emergenze, garantisca con essa opportuni canali di comunicazione. A tale scopo potrebbe essere utile pubblicare sul sito i riferimenti (*mail*) per comunicare con l'organo di controllo.

Casistica 2

In questo ambito e contesto sarebbe opportuno attivare azioni di controllo di costante conformità in riferimento a bandi, disposizioni di dettaglio e in riferimento al dettato del Regolamento (UE) N. 1303/2013 del Parlamento Europeo e del Consiglio del 17 dicembre 2013 recante disposizioni generali sul Fondo Europeo di Sviluppo Regionale, sul Fondo Sociale Europeo e sul Fondo di Coesione.

In particolare, al fine di presidiare correttamente il flusso finanziario ed economico relativo ai progetti, si ritiene necessario formalizzare la prassi esistente introducendo una procedura che descriva modalità operative e controlli delle attività economiche e finanziarie dei progetti, dalla progettazione fino alla rendicontazione del corso e sua chiusura; la procedura, che dovrà essere verificata e approvata dall'O.d.V., dovrà essere chiara ed esaustiva circa le attribuzioni di responsabilità e autorità per la gestione delle attività e dei controlli e deve prevedere specifiche attività di *auditing* periodico attuato dallo stesso O.d.V..

L'O.d.V., come prevede sia la Parte Generale A, sia il proprio Regolamento, consuntiva annualmente lo stato dell'arte e dispone aggiornamenti nella valutazione di questa fattispecie di commissione reato.

A completamento delle attività devono essere effettuate periodiche azioni formative e informative ai dipendenti in modo che siano in grado di gestire le attività sul tema del controllo economico dei progetti e possano conoscere i contenuti del Codice Etico e del Regime Sanzionatorio.

Casistica 3

Le attività di licitazione e gare ad affidamento diretto sono gestite direttamente dalla Divisione Gare PA in collaborazione con le Filiali. In questo ambito la Divisione Gare PA, come prevede la Procedura del Sistema Qualità PRO Gare alla quale in questa sede si rimanda, deve trasmettere adeguate informazioni alla Sede centrale (AMM) e, conseguentemente, all'O.d.V. stesso che può, a campione, effettuare controlli di conformità.

Soprattutto, nell'ambito degli affidamenti diretti e nei casi di cui alla Procedura PRO Gare, è necessario un controllo da parte della Sede centrale con adeguata e tempestiva comunicazione all'organo di controllo (O.d.V.). Tale controllo ha la finalità di individuare e scongiurare elementi di commistione tra Stazione Appaltante e rappresentante di Etjca specie se operativo in aree delocalizzate rispetto alla Sede centrale.

Casistiche 1, 2 e 3. Gestione delle informazioni verso l'O.d.V. e gestione del programma di *audit*.

Si dispone che i responsabili trasmettano all'O.d.V. documenti ritenuti rilevanti riconducibili a: controlli, sopralluoghi, ispezioni, *audit*, verbali, ecc. condotti da funzionari della P.A. o incaricati di pubblico servizio. Nel caso di riscontri negativi (situazioni anomale all'O.d.V. sullo stato dei rapporti con le Autorità pubbliche di Vigilanza) la comunicazione verso l'O.d.V. deve essere immediata utilizzando al riguardo il Modello Allegato G; altrimenti tutta la documentazione dovrà essere trasmessa come descritto nella tabella riassuntiva (in ogni caso prima dell'*audit* periodico e del consuntivo annuale da parte dell'O.d.V.). A tale scopo, in entrambi i casi, il responsabile designato trasmette il Mod. Allegato F - Notifica Controlli.

Uno specifico Protocollo individua le modalità di trasmissione degli atti all'O.d.V. mentre una procedura individua modalità per la gestione delle informazioni riconducibili ai flussi economici con la P.A.

Inoltre, ETJCA prevede di gestire uno specifico programma di *audit* periodici allo scopo di verificare l'adeguatezza del sistema di interno che regolamenta i rapporti con i soggetti della PA (siano essi addetti al controllo e monitoraggio, siano essi Enti Finanziatori e Regolatori nell'ambito dell'approvazione di progetti e nella fase di rendi/resocontazione e liquidazione delle spettanze). Questo programma, che deve essere completato prima della relazione Annuale, viene gestito dall'O.d.V. è si articola nelle seguenti fasi:

- definizione piano di *audit* annuale al fine di valutare il rispetto del modello organizzativo;
- nomina del/degli *auditor* (di solito il membro specialista dell'O.d.V.);
- svolgimento dell'audit secondo le tempistiche concordate;
- redazione verbale con segnalazione delle difformità riscontrate.

Inoltre, resta valida la prassi di trametterе periodicamente all'O.d.V. gli esiti derivanti dalla compilazione a cura dei responsabili di Sede delle Liste di Riscontro: Allegato B – Check-list Stato Filiali e Allegato E – Check-list Sede Centrale. Unitamente alla documentazione di *audit e alle Check-list* di Autovalutazione (Allegati B ed E), *l'auditor* incaricato dovrà acquisire tutta la documentazione pertinente (verbali di monitoraggio, verifiche di accreditamento, sopralluoghi, controlli, fatture emesse, ecc.). Tutta la documentazione di *audit* appena indicata dovrà essere trasmessa al Committente (O.d.V.) prima della Relazione Annuale.

Schema riassuntivo di misure e procedure

Casistica	Responsabile	Descrizione attività di controllo, risorse, strumenti
1	Direzione	Applicazione di specifica Procedura di controllo del processo economico/finanziario dei progetti con chiare attribuzioni di compiti, responsabilità, autorità, deleghe a operare e chiari riferimenti alla tracciabilità dei flussi economici e bancari.
2	Direzione	Applicazione di specifico Protocollo con chiare attribuzioni di compiti, responsabilità, autorità a operare e interloquire con incaricati dalla P.A. (Funzionari o Incaricati di Pubblico Servizio).
1 e 2	Direzione	Formazione e informazione Funzioni coinvolte.
1 e 2	Direzione	Condivisione Codice Etico e Regime Sanzionatorio.
1 e 2	*Area Developer* Responsabili di Progetto	Utilizzando il Modello Allegato F - Notifica Controlli, trasmissione mensile al *Manager* Politiche Attive di atti e documenti rilevanti quali, per es.: verbali di controllo di soggetti della PA e incaricati di Pubblico Servizio. Trasmissione immediata di esiti negativi o difformi utilizzando il Modello Allegato G.
1 e 2	*Manager* Politiche Attive	Rendicontazione semestrale all'O.d.V. in merito ai controlli interni ed esterni (effettuati dagli Uffici competenti). Immediata trasmissione nel caso di provvedimenti, criticità ecc..
1	O.d.V.	Organizzazione di canali d'informazione tra O.d.V. e Dirigente Responsabile Ufficio P.A.
1 e 2	Divisione Formazione	Rendicontazione semestrale all'O.d.V. in merito ai controlli interni ed esterni (effettuati dagli Uffici competenti). Immediata trasmissione nel caso di provvedimenti, criticità ecc..
3	Divisione PA	Informativa periodica a O.d.V. in merito a partecipazione a gare/licitazioni e relativi esiti e gestione
1, 2 e 3	O.d.V.	Organizzazione di canali d'informazione tra O.d.V. e parti interessate su casi ritenuti a rischio in applicazione della Procedura PRT 03 - Protocollo segnalazioni di illeciti e irregolarità
1 e 2	O.d.V.	Azioni di *Auditing* periodico (almeno un *audit*/anno) e possibilità di verifiche senza preavviso
1 e 2	O.d.V.	Acquisire Liste di Riscontro: All. B - Check-list Stato Filiali e All. E - Check-list Sede Centrale
1 e 2	O.d.V.	Acquisire documenti e informazioni in merito all'efficacia delle azioni adottate, eventualmente prescrivere azioni integrative e informare il vertice aziendale.
1 e 2	O.d.V.	Redazione di Piano Annuale e consuntivo su Relazione Finale (§ 7 Parte Generale)

CAPITOLO 2: Reati Societari

2.1 – Principali riferimenti normativi

Articoli di Legge	Cod.
art. 2621 c.c.: false comunicazioni sociali	2.1
art. 2622 c.c.: false comunicazioni sociali in danno dei soci o dei creditori	2.2
art. 2623, primo comma, c.c.: falso in prospetto	2.3
art. 2624, primo comma, c.c.: falsità nelle relazioni o nelle comunicazioni delle società di revisione	2.4
art. 2625, secondo comma, c.c. impedito controllo	2.5
art. 2632 c.c. formazione fittizia del capitale	2.6
art. 2626 c.c. indebita restituzione dei conferimenti	2.7
art. 2627 c.c. illegale ripartizione degli utili e delle riserve	2.8
art. 2628 c.c. illecite operazioni sulle azioni o quote sociali o della società controllante	2.9
art. 2629 c.c. operazioni in pregiudizio dei creditori	2.10
art. 2633 c.c. indebita ripartizione dei beni sociali da parte dei liquidatori	2.11
art. 2636 c.c. illecita influenza sull'assemblea	2.12
art. 2637 c.c. aggiotaggio	2.13
art. 2629 bis c.c. omessa comunicazione del conflitto d'interessi	2.14
art. 2638 c.c. ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza e delle funzioni delle autorità pubbliche di vigilanza	2.15
manipolazione del mercato (art. 185 T.U.I.F.);	2.16
abuso di informazioni privilegiate (art. 184 T.U.I.F.)	2.17
D.Lgs. n. 61/2002 in materia di falso in bilancio e false comunicazioni sociali	2.18
Legge 27 maggio 2015, n. 69 - Disposizioni in materia di delitti contro la pubblica amministrazione, di associazioni di tipo mafioso e di falso in bilancio	2.19

2.2 – Analisi iniziale

Il Sistema di prevenzione dei reati societari deve poter gestire il rischio residuo sulla base di un'analisi dello stato dell'arte in funzione degli obiettivi societari, degli eventi di origine interna e esterna che possono pregiudicare il conseguimento degli obiettivi e dell'ambiente interno; in questo ultimo caso il *management* formula la filosofia di base e determina il livello di accettabilità del rischio.

Destinatari del presente Capitolo sono: l'amministratore e i sindaci ("soggetti apicali") di ETJCA S.p.A., nonché i dipendenti soggetti a vigilanza e controllo da parte dei soggetti apicali nelle sottoelencate aree di attività a rischio, qui di seguito tutti denominati "Destinatari". Per quanto concerne gli amministratori la legge equipara a coloro che sono formalmente investiti di tali qualifiche anche i soggetti che svolgono tali funzioni "di fatto". Ai sensi dell'art. 2639 c.c., infatti, dei reati societari previsti dal codice civile, risponde sia chi è tenuto a svolgere la stessa funzione, diversamente qualificata, sia chi esercita in modo continuativo e significativo i poteri tipici inerenti alla qualifica o alla funzione.

Il vigente sistema di formazione del bilancio e il relativo controllo del processo di comunicazione sociale è, allo stato attuale, conforme alle vigenti disposizioni normative ma è necessario riesaminare l'efficacia di esso partendo da un'attenta analisi iniziale volta a individuare eventuali elementi di carenza e di fattori di rischio latenti da limitare o, se possibile, eliminare. Più specificamente le aree di attività ritenute a rischio in relazione ai reati societari sono considerate le seguenti:

- Predisposizione della bozza di bilancio e delle situazioni infra-annuali;
- Gestione fatturazione attiva/passiva;
- Gestione risorse finanziarie;
- Gestione tesoreria, rimborsi spesa;
- Comunicazione e svolgimento delle assemblee e gestione dei rapporti con il Collegio Sindacale;
- Gestione recupero crediti;
- Gestione amministrativa del personale (Sede, Filiali, somministrati);
- Gestione dei rapporti con Organi Ispettivi;
- Operazioni aventi ad oggetto strumenti finanziari.

Oltre a quanto appena specificato, il D.Lgs. n. 61/2002 ha previsto l'inserimento nel decreto 231 di specifiche sanzioni a carico dell'ente in relazione a reati in materia societaria previsti dal codice civile.

La predisposizione di un modello di organizzazione in questo contesto, oltre ad assumere un'importante valenza probatoria della volontà della Società di eliminare i difetti di organizzazione che possano facilitare la commissione di determinati illeciti, può assicurare sia una corretta gestione dei proventi derivanti da attività con la PA (es. Attività Garanzia Giovani, altri progetti di Politiche Attive del Lavoro), sia un'accresciuta trasparenza delle procedure e dei processi interni e, quindi, maggiori possibilità di controllo sull'operato degli organi societari.

Da ciò nasce dunque la duplice esigenza di: a) approntare specifiche misure organizzative e procedurali atte a fornire ragionevole garanzia di prevenzione di questa tipologia di reati; b) individuare compiti di *auditing* e controllo dell'Organismo di Vigilanza per assicurare l'effettivo, efficace, efficiente e continuo funzionamento del modello stesso.

La seguente matrice identifica le aree aziendali (funzioni e processi) oggetto di indagine in riferimento ai rischi specifici.

Funzioni/Aree	Processi, fasi e attività	N. casistica
C.d.A./ Collegio Sindaci	Processo di formazione del bilancio e relativi controlli e di gestione delle comunicazioni sociali	1

Processo **Processi C.d.A.**				Giudizio Preliminare [2]	Controlli Esistenti						Valutazione Controlli [3]	Ruolo della Funzione					
Sigla Area/Funz.	N. Fase/Attività	Cod. Reato	Fattore [1]		Esistenza di Procedure	Aggiornamento Procedure	Esistenza di Deleghe	Conoscenza e Comunicazione	Suddivisione Compiti	Controlli e Monitoraggi		Operativo	Decisionale	Autorizzativo	Monitoraggio	Sanzionatorio	*Training*
C.d.A.	1	2	I, D	M	☑	☑	☑	☑	☑	☑	M	☑	☑	☑	☒	☑	☒
SND	1	2	I, D	M	☑	☑	☑	☑	☑	☑	M	☑	☒	☒	☑	☒	☒

1 I = Interno, E = Esterno, D = Decisionale. **2** Giudizio preliminare rischio reato: A = Alto, M = Medio, B = Basso, I = Inesistente. **3** Valutazione efficacia e adeguatezza dei controlli: I = Inefficaci, M = da migliorare, E = Efficaci, N = Non Esistenti. 4 ☒ = Elemento non presente; ☑ = Elemento Presente.

2.3 – Valutazione del Rischio

Modalità e contesti di commissione del reato

Alla luce del processo di adozione del Modello e in particolare delle attività di *risk assessment* sono state ritenute significative o potenzialmente significative ai fini dell'attuazione del Decreto le seguenti attività sensibili:

1. la predisposizione di comunicazioni dirette al Consiglio di Amministrazione e ai Soci riguardo la situazione economica, patrimoniale e finanziaria di Etjca S.p.A., anche nel caso in cui si tratti di comunicazioni diverse dalla documentazione contabile periodica (bilancio d'esercizio, *budget* generale delle attività, cash-flow, ecc.);
2. la predisposizione e divulgazione verso l'esterno di dati o notizie (ulteriori rispetto a quelli sulla situazione economica, patrimoniale e finanziaria di cui al punto 1).

La commissione dei reati riconducibili al falso in bilancio e falso nelle comunicazioni sociali potrebbe delinearsi, in applicazione della legge 69/2015, come comportamento commissivo oppure come comportamento omissivo di comunicazioni obbligatorie previste dalla Legge.

La situazione relativa al secondo caso non dovrebbe porre problemi sia perché la prevenzione del rischio in questo senso è una derivazione della corretta gestione economica e finanziaria della Società di cui al punto 1, sia perché esiste il controllo previsto dalla legge esercitato dai Sindaci.

Rischi e ricadute

I rischi sono riconducibili alla situazione contabile generale e al controllo dei flussi economici e finanziari nell'ambito di attività a libero mercato o finanziate. In questo contesto una cattiva gestione delle attività contabili e finanziarie porterebbe a conseguenze pericolose per l'equilibrio economico in sé, ma anche conseguenze negative in relazione al mercato del lavoro, allo stato di accreditamento regionale e anche come immagine verso i portatori d'interesse esterni e la stessa PA.

Controlli esistenti

Esiste un sistema di controllo interno previsto dallo Statuto che consente una suddivisione di compiti e specifiche responsabilità, autorità e deleghe. Inoltre, lo Statuto prevede azioni di controllo svolte da parte dei Sindaci che di fatto controllano e avvallano la situazione contabile. Il Bilancio d'esercizio viene approvato dal Consiglio di Amministrazione previa verifica da parte dei Sindaci e successiva certificazione del documento contabile e finanziario da parte della Società incaricata della certificazione del bilancio.

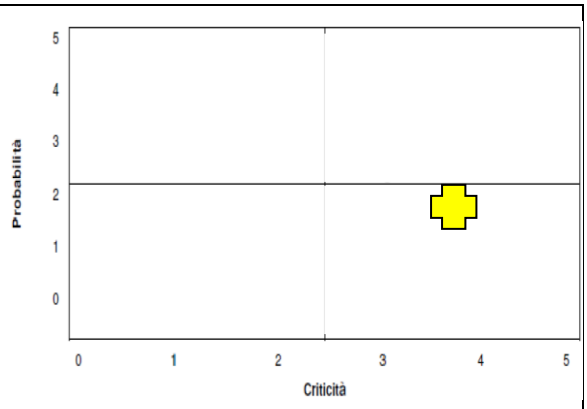
Più da un punto di vista operativo esiste una consolidata prassi autorizzativa delle spese che individua responsabilità separate rispetto a chi dispone ordinativi e chi materialmente li esegue e li verifica.

Di conseguenza, considerando il rapporto costi/benefici, il posizionamento dell'indice di valutazione si trova in un'area intermedia in termini di probabilità di accadimento.

Quantificazione del Rischio

Nell'ambito dei singoli rischi di reato, potenzialmente attivi in specifiche aree aziendali, se ne valuta la *magnitudo* sulla base delle variabili: probabilità e impatto e, in relazione al valore ottenuto e agli scostamenti, si definisce un piano operativo definendo le tipologie di misure preventive e di controllo da attuare.

Probabilità							
Molto alta	0,45	0,00	2,25	4,50	9,00	18,00	36,00
Alta	0,35	0,00	1,75	3,50	7,00	14,00	28,00
Media	0,25	0,00	1,25	2,50	5,00	10,00	20,00
Bassa	0,15	0,00	0,75	1,50	3,00	6,00	12,00
Molto bassa	0,05	0,00	0,25	0,50	1,00	2,00	4,00
Nulla	0,00	0,00	0,00	0,00	0,00	0,00	0,00
		0	5	10	20	40	80
		Nullo	Molto basso	Basso	Medio	Alto	Molto alto
		Impatto					



Probabilità	Impatto	Indice di Valutazione:
0,15	**40**	**6**

La Magnitudo si ottiene moltiplicando le variabili P e I (**M = P * I**); da cui ne deriva che l'Esposizione che può essere classificata **Bassa**, **Media** o **Elevata**. Strategie di *risk response*. Per un rischio alto: **evitare** il rischio (*risk avoidance*), per un rischio medio: **limitare** il rischio (*risk reduction*) o **trasferire** il rischio (*risk transferring/sharing*), per il rischio basso: **accettare** il rischio (*risk acceptance*).

2.4 – Misure e Procedure

L'operatività delle attività sensibili rispetto ai reati societari dovrà uniformarsi ai seguenti criteri:

1) rigoroso rispetto delle norme di legge, dei regolamenti e delle procedure aziendali applicabili e piena trasparenza nella gestione di tutte le attività:

a) che possano incidere sull'integrità del capitale sociale, o su ogni altro presidio previsto dalle norme o dalle procedure interne a garanzia dei creditori;
b) funzionali alla formazione e redazione dei bilanci e di ogni comunicazione sociale, relazione, prospetto previsti dalle norme, rappresentando e comunicando tempestivamente, correttamente e con completezza i dati e le informazioni inerenti alla situazione finanziaria, patrimoniale ed economica della Società;
c) finalizzate a garantire il corretto funzionamento e la capacità operativa degli organi sociali, con particolare riferimento alla libera formazione ed espressione della volontà dell'assemblea, omettendo ogni atto, informazione o rappresentazione fraudolenta o simulata che possa influenzare scorrettamente tale volontà;

2) completa, efficace, propositiva e tempestiva collaborazione e trasparenza nei rapporti e nelle comunicazioni con gli organi (interni ed esterni) deputati al controllo ed alla vigilanza delle diverse funzioni impegnate nella gestione degli adempimenti societari, omettendo ogni comportamento atto – direttamente o indirettamente – a impedire, ostacolare o deviare, mediante artificiosa alterazione di dati e informazioni, l'esecuzione delle operazioni di controllo e di revisione.

Più in generale è necessario che l'O.d.V., attraverso attività strutturate di *reporting* e di *auditing* (eventualmente commissionate a professionisti esterni), verifichi che non si realizzino le seguenti condizioni:

- rappresentare o trasmettere per l'elaborazione dei bilanci, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, ovvero predisporre comunicazioni sociali dirette al socio o al pubblico che non rappresentino in modo veritiero la situazione economica, patrimoniale e finanziaria della Società;
- omettere dati e informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria;
- restituire conferimenti al socio o liberare lo stesso dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;
- ripartire utili o acconti su utili non effettivamente conseguiti o da destinarsi per legge a riserva;
- acquistare o sottoscrivere quote della Società o azioni della società capogruppo fuori dai casi previsti dalla legge, con lesione all'integrità del capitale sociale;
- effettuare riduzioni del capitale sociale, fusioni o scissioni, in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno;
- procedere a formazione o aumento fittizio del capitale sociale, attribuendo azioni per un valore inferiore al loro valore nominale in sede di aumento del capitale sociale;
- distrarre i beni sociali, in sede di liquidazione della società, dalla loro destinazione ai creditori, ripartendoli fra i soci prima del pagamento dei creditori o dell'accantonamento delle somme necessarie a soddisfarli;
- esporre nelle comunicazioni ad Autorità Amministrative Indipendenti fatti non rispondenti al vero, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie della Società;
- attuare comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che comunque costituiscano ostacolo allo svolgimento all'attività di controllo o di revisione della gestione sociale da parte del Collegio Sindacale o della società di revisione;
- determinare o influenzare l'assunzione delle deliberazioni dell'assemblea, attuando atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare
- attuare qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni delle Autorità Amministrative Indipendenti, anche in sede di ispezione (a titolo esemplificativo: espressa opposizione, rifiuti pretestuosi, o anche comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti).

L'Organismo di Vigilanza ha la possibilità di effettuare due tipologie di controlli (il primo dei quali è obbligatorio).

A) effettuare controlli a campione sulle attività connesse ai «processi sensibili» diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello. A tal fine all'Organismo viene garantito libero accesso a tutta la documentazione aziendale rilevante così come previsto nella Parte Generale del Modello 231. Inoltre, l'Organismo di Vigilanza può attivarsi con specifici controlli a seguito delle segnalazioni ricevute, secondo quanto riportato nella Parte Generale del Modello 231.

B) Gestire uno specifico programma di *audit* periodici allo scopo di verificare l'adeguatezza del sistema interno che regolamenta il contesto economico e finanziario. Questo programma, che deve essere completato prima della relazione Annuale, viene gestito dall'O.d.V. è si articola nelle seguenti fasi:

- definizione piano di *audit* annuale al fine di valutare il rispetto del modello organizzativo;
- nomina del/degli *auditor* (di solito il membro specialista dell'O.d.V.);
- svolgimento dell'audit secondo le tempistiche concordate (per la conduzione della verifica sul campo è possibile utilizzare al riguardo l'Allegato A – Check-list reati Societari);
- redazione verbale con segnalazione delle difformità riscontrate.

Inoltre, resta valida la prassi di trametterе periodicamente all'O.d.V. gli esiti derivanti dalla compilazione, a cura dei Responsabili, di Sede delle Liste di Riscontro: Allegato B – Check-list Stato Filiali e Allegato E – Check-list Sede Centrale. Unitamente alla documentazione di *audit e alle Check-list* di Autovalutazione (Allegati B ed E), *l'auditor* incaricato dovrà acquisire tutta la documentazione pertinente. Tutta la documentazione di *audit* appena indicata dovrà essere trasmessa al Committente (O.d.V.) prima della Relazione Annuale.

Per tutto quanto fino a questo punto scritto oltre ai controlli di prassi esistenti è necessario condividere principi e modalità operative mediante l'applicazione del Protocollo contenente i principi di comportamento utili alla prevenzione di comportamenti commissivi o omissivi in ordine ai reati societari; inoltre è opportuno verificare periodicamente il corretto conferimento di precise, responsabilità, autorità, compiti e deleghe formalmente approvate degli Organi societari.
Prevedere inoltre periodiche attività di formazione di base verso tutti i responsabili affinché conoscano le principali nozioni in tema di reato di corruzione privata (in particolare norme di legge, sanzioni, fattispecie a rischio reato).

In relazione a eventuali conflitti d'interesse di figure apicali o di dipendenti è importante verificare sempre l'adeguatezza del modello organizzativo interno e del sistema delle responsabilità. Eventualmente potrebbero essere utili procedure autorizzative per operazioni esposte a situazioni di conflitto di interesse evidenziate da singoli amministratori o anche la previsione di un meccanismo di segnalazione tempestiva ai superiori di qualsiasi situazione di conflitto di interessi che possa insorgere in capo a soggetti e relative modalità di intervento.

In aggiunta è necessario prevedere uno specifico strumento per le comunicazioni di situazioni anomale all'O.d.V. (si utilizzi al riguardo il Modello Allegato G).

Oltre a ciò, si conferma la validità e la necessità di condividere il Codice Etico e Regime Sanzionatorio.

Anche in questo caso l'O.d.V., come prevede sia la Parte Generale A, sia il proprio Regolamento, consuntiva annualmente lo stato dell'arte e dispone aggiornamenti nella valutazione di questa fattispecie di commissione reato.

Schema riassuntivo di misure e procedure

Casistica	Responsabile	Descrizione attività di controllo, risorse, strumenti
1	Direzione	Condivisione Codice Etico e Regime Sanzionatorio.
1	Direzione	Formazione/informazione specifica per il personale
1	Direzione	Definizione di specifico Protocollo con specifiche regole di prevenzione reati
1	Direzione/AMM	Trasmissione dei documenti rilevanti da un punto di vista contabile.
1	Direzione/AMM	Trasmissione del *report* di certificazione del bilancio e relativi esiti
1	O.d.V.	Riesame di documenti rilevanti da un punto di vista delle procedure e responsabilità interne e della documentazione contabile.
1	O.d.V.	Trasmissione *report* sulle attività di controllo espletate e sulla loro efficacia e sull'efficacia del Sistema di prevenzione dei reati societari
1	O.d.V.	Incontri con il Collegio Sindacale e con il C.d.A. per consultare gli esiti delle relazioni al fine di identificare aree e/o settori dove le due funzioni di controllo citate possono aver riscontrato anomalie o procedure inefficaci o inefficienti. L'O.d.V. può eventualmente prescrivere azioni integrative.
1	O.d.V.	Attività di *auditing* annuale commissionata dall'O.d.V. a professionista esterno o condotta da un componente dell'O.d.V. stesso
1	O.d.V.	Acquisire Liste di Riscontro: All. B - Check-list Stato Filiali e All. E - Check-list Sede Centrale
1	O.d.V.	Redazione di Piano Annuale e consuntivo su Relazione Finale (§ 7 Parte Generale)
1, 2 e 3	O.d.V.	Organizzazione di canali d'informazione tra O.d.V. e parti interessate su casi ritenuti a rischio in applicazione della Procedura PRT 03 - Protocollo segnalazioni di illeciti e irregolarità

CAPITOLO 3: Reati di Abuso di Mercato

3.1 – Principali riferimenti normativi

Articoli di Legge	Cod.
Abuso di informazioni privilegiate e di manipolazione del mercato previsti dalla parte V, titolo I-bis, capo II, del Testo Unico di cui al decreto legislativo 24 febbraio 1998, n. 58	3.1

3.2 – Analisi iniziale

La matrice seguente identifica le aree aziendali (funzioni e processi) oggetto di indagine in riferimento ai rischi specifici.

Funzioni/Aree	Processi, fasi e attività	N. casistica
Uff. Contratti	Erogazione dei servizi presso i clienti	1

Processo: **Erogazione dei servizi ai clienti**				Giudizio Preliminare [2]	Controlli Esistenti						Valutazione Controlli [3]	Ruolo della Funzione					
Sigla Area/Funz.	N. Fase/Attività	Cod. Reato	Fattore [1]		Esistenza di Procedure	Aggiornamento Procedure	Esistenza di Deleghe	Conoscenza e Comunicazione	Suddivisione Compiti	Controlli e Monitoraggi		Operativo	Decisionale	Autorizzativo	Monitoraggio	Sanzionatorio	*Training*
C	1	3.1	I, E	B	☒	☒	☒	☒	☒	☒	N	☒	☑	☒	☒	☑	☒

Annotazioni. L'analisi iniziale indica che le misure e i controlli sono praticamente inesistenti; tale contesto trova tuttavia la sua giustificazione nel fatto che l'entità del rischio è comunque da considerarsi bassa. Sebbene la Società non risulti quotata in borsa su mercati finanziari, tuttavia i reati in oggetto sono di natura "comune" e cioè possono essere compiuti da ogni persona indipendentemente dal possesso di particolari qualifiche, deleghe o responsabilità. Peraltro, l'ordinamento punisce espressamente, oltre ai membri del C.d.A., anche il professionista/lavoratore che, nell'esercizio dell'attività lavorativa, abusi di informazioni diffondendo o divulgando notizie, dati e informazioni privilegiate di cui si è venuti a conoscenza in occasione delle attività svolte presso il Cliente.

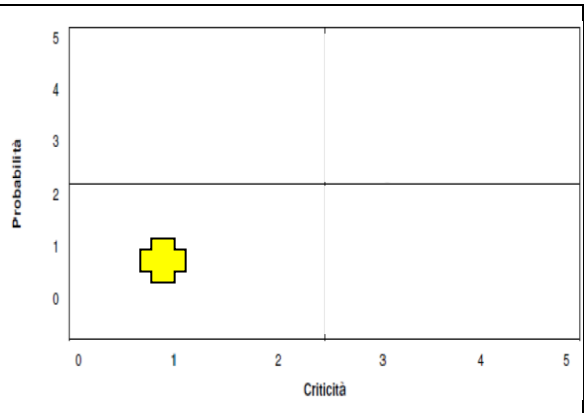
1 I = Interno, E = Esterno, D = Decisionale. **2** Giudizio preliminare rischio reato: A = Alto, M = Medio, B = Basso, I = Inesistente. **3** Valutazione efficacia e adeguatezza dei controlli: I = Inefficaci, M = da migliorare, E = Efficaci, N = Non Esistenti. 4 ☒ = Elemento non presente; ☑ = Elemento Presente.

3.3 – Valutazione del Rischio

Nell'ambito dei singoli rischi di reato potenzialmente attivi, in ognuna delle aree aziendali analizzate, se ne valuta la *magnitudo* di ognuno di essi sulla base delle variabili: probabilità e impatto e, sulla base del valore ottenuto e degli scostamenti, si definisce un piano operativo definendo innanzitutto le tipologie di misure preventive e di controllo da attuare.

Si consideri l'Area Contratti nell'ambito del processo di Erogazione dei servizi presso i clienti.

Probabilità							
Molto alta	0,45	0,00	2,25	4,50	9,00	18,00	36,00
Alta	0,35	0,00	1,75	3,50	7,00	14,00	28,00
Media	0,25	0,00	1,25	2,50	5,00	10,00	20,00
Bassa	0,15	0,00	0,75	1,50	3,00	6,00	12,00
Molto bassa	0,05	0,00	0,25	0,50	1,00	2,00	4,00
Nulla	0,00	0,00	0,00	0,00	0,00	0,00	0,00
		0	5	10	20	40	80
		Nullo	Molto basso	Basso	Medio	Alto	Molto alto
		Impatto					



Probabilità	Impatto	Indice di Valutazione:
0,05	**10**	**0,50**

La Magnitudo si ottiene moltiplicando le variabili P e I (**M = P * I**); da cui ne deriva che l'Esposizione che può essere classificata **Bassa**, **Media** o **Elevata**. Strategie di *risk response*. Per un rischio alto: **evitare** il rischio (*risk avoidance*), per un rischio medio: **limitare** il rischio (*risk reduction*) o **trasferire** il rischio (*risk transferring/sharing*), per il rischio basso: **accettare** il rischio (*risk acceptance*).

Annotazioni sulla valutazione. Si decide di attribuire una magnitudo del rischio bassa e, di conseguenza, la natura dei controlli deve essere commisurata al non elevato livello del rischio. È possibile accettare il rischio residuale ma è anche possibile attuare un automatico e non gravoso controllo in fase contrattuale per essere al riparo da rischi latenti.

3.4 – Misure e Procedure

Sebbene il rischio sia residuale, tuttavia, sulla base dei riscontri dell'analisi iniziale, si stabiliscono le specifiche azioni preventive, gli strumenti/risorse e le relative responsabilità.

Casistica	Responsabile	Descrizione attività di controllo, risorse, strumenti
1	O.d.V.	Consegnare/esporre/pubblicare il Codice Etico anche a collaboratori esterni.
1	O.d.V.	Formazione/informazione specifica per il personale
1	Uff. Contratti	Il rischio residuale può essere gestito in fase contrattuale richiedendo la sottoscrizione da parte di collaboratori, consulenti e dipendenti della Società dell'impegno a non diffondere o divulgare notizie, dati e informazioni privilegiate di cui si è venuti a conoscenza in occasione delle attività svolte presso il Cliente.
1	O.d.V.	L'O.d.V. deve acquisire informazioni in merito all'efficacia delle azioni adottate, eventualmente prescrivere azioni integrative e informare il Vertice aziendale.
1	O.d.V.	Redazione di Piano Annuale e consuntivo su Relazione Finale (§ 7 Parte Generale)

CAPITOLO 4: Reati Informatici e reati contro la *privacy*

4.1 – Principali riferimenti normativi

Articoli di Legge	Cod.
Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. D.Lgs. D.Lgs. 196/03 - Testo Unico sulla tutela delle persone e di altri soggetti al trattamento dei dati personali	4.1
art. 640 *ter* c.p.; frode informatica	4.2
art. 615 *ter* c.p., accesso abusivo a un sistema informatico o telematico	4.3
art. 615 *quater* c.p., detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici	4.4
art. 615 *quinquies* c.p., diffusione di programmi diretti a danneggiare o interrompere un sistema informatico	4.5
art. 617 *quater* c.p., intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche	4.6
art. 617 *quinquies* c.p., installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche	4.7
art. 635 *bis* c.p., danneggiamento di sistemi informatici e telematici	4.8
art. 635 *ter* c.p., danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità	4.9
art. 635 *quater* c.p., danneggiamento di sistemi informatici o telematici	4.10
art. 635 *quinquies* c.p., danneggiamento di sistemi informatici o telematici di pubblica utilità	4.11
art. 491 *bis* c.p., falsità in documenti informatici	4.12
art. 640 *quinquies* c.p., frode informatica del soggetto che presta servizi di firma elettronica	4.13
Legge n. 238/2021; Direttive n. 2013/40/UE e n. 2011/93/UE.	4.14

4.2 – Analisi iniziale

L'articolo 24-bis del decreto 231 ha esteso la responsabilità amministrativa delle persone giuridiche e degli enti alla quasi totalità dei reati informatici. Alla luce dei presupposti applicativi del decreto, i soggetti economici sono considerati responsabili per i delitti informatici commessi nel loro interesse o a loro vantaggio da persone che rivestono funzioni di rappresentanza, amministrazione, direzione dell'ente o di una sua unità organizzativa, ma anche da persone sottoposte alla loro direzione o vigilanza. Le tipologie di reato informatico si riferiscono a una molteplicità di condotte criminose in cui un sistema informatico risulta, in alcuni casi, obiettivo stesso della condotta e, in altri, obiettivo stesso della condotta e, in altri, lo strumento attraverso cui l'autore intende realizzare altra fattispecie penalmente rilevante.

Lo sviluppo della tecnologia informatica ha generato nel corso degli anni modifiche sostanziali nell'organizzazione del *business* e ha inciso sensibilmente sulle opportunità a disposizione di ciascun responsabile di area o funzione per realizzare o occultare non soltanto schemi di condotte criminali già esistenti ma anche fattispecie nuove, tipiche del cd. mondo virtuale. A ciò si aggiunga l'ingresso massivo di dispositivi mobili (es. *tablet* e *smartphone*), l'utilizzo di *server* di *cloud computing* (per esempio servizi di memorizzazione e archiviazione dei dati distribuiti su reti e server remoti) che di fatto moltiplicano le opportunità di realizzazione di un reato informatico, introducono criticità in relazione al loro utilizzo aziendale in virtù dei ridotti interventi del legislatore e determinano la necessità per le imprese di adeguarsi rapidamente al fine di disciplinare correttamente la gestione di tali fenomeni.

Quanto ai soggetti maggiormente esposti a tale fattispecie di reato, tale fenomeno può coinvolgere qualsiasi ente che utilizzi in maniera rilevante gli strumenti informatici e telematici per lo svolgimento delle proprie attività.

La Legge n. 238/2021, pubblicata in Gazzetta Ufficiale lo scorso 17 gennaio ed entrata in vigore il 1° febbraio 2022, in un'ottica di uniformazione delle previsioni di diritto nazionale alle richieste del diritto europeo, è intervenuta apportando significative modifiche ad alcune fattispecie del Codice penale, rientranti nell'alveo dei reati presupposto di cui al D.Lgs. 231/2001. Nello specifico, le linee di intervento possono essere identificate nell'adeguamento alla Direttiva n. 2013/40/UE relativa agli attacchi contro i sistemi di informazione - modifica degli artt. 615 e ss. c.p., richiamati dall'art. 24-bis del D.Lgs. 231/2001.

Si segnalano al riguardo le modifiche apportate a talune fattispecie richiamate come reati presupposto dall'art. 24-bis del D.Lgs. 231/2001, dedicato ai "Delitti informatici e trattamento illecito di dati". In particolare, l'articolo 615-quater c.p., prevede un ampliamento delle condotte punibili e una modificazione in termini di cornice edittale. La nuova disposizione, rubricata ora "Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici", prevede che sia punibile il soggetto che "abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza al fine di arrecare a sé o ad altri un profitto o di arrecare ad altri un danno". La pena

della reclusione si estende sino a due anni nell'ipotesi base, mentre da uno a tre anni se ricorre una delle circostanze di cui all'articolo 617- quater comma 4.

L'articolo 615-quinquies c.p. ora rubricato "Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico" e così come modificato dalla suddetta legge, si connota per una nuova formulazione della condotta punibile ora rivolta a "Chiunque, allo scopo 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, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329".

Con riferimento all'art. 617-quater c.p., vengono inasprite le pene per l'ipotesi di cui al primo comma ora punita con la reclusione "da un anno e sei mesi a cinque anni", nonché di quella prevista dal comma quarto per la quale si prevede un innalzamento della pena edittale "da tre a otto anni".

L'articolo 617-quinquies ora rubricato "Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche" si connota per una nuova formulazione relativa alle condotte punibili che prevedono ora l'attivazione della risposta sanzionatoria nei confronti di chiunque "procuri, detiene, produca, riproduca, diffonda, importi, comunichi, consegni, metta in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi atti ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi" con il fine di "intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle".

Analisi relativa ai processi gestiti da Etjca S.p.A. Si considerino due livelli di operatività. L'attività lato *server* (gestionale) e l'attività di Filiale operata sulle singole postazioni. Lato *server* sono implementati i controlli di sicurezza (accessi fisici e logici ai dati e fruizione degli stessi) di classe *enterprise* considerata anche l'importanza centrale dei sistemi stessi. Nelle attività svolte presso le Filiali, o comunque sulle postazioni PC personali, sono attuati controlli in conformità alle disposizioni di legge (esistono *password* di accesso, sistemi attività di *backup*, protezione da virus, *firewall*, ecc.); tuttavia i processi gestiti presso le filiali non rappresentano elemento critico ai fini dell'operatività aziendale e della sicurezza.

La matrice identifica le aree aziendali (funzioni e processi) oggetto di indagine in riferimento ai rischi specifici.

Funzioni/Aree	Processi, fasi e attività	Casistica
Risorse Umane/ Responsabile dei Sistemi Informativi e DPO	Trattamento dei dati individuali sensibili e ordinari	1
Dipendente della società	Utilizzo del Sistema Informativo interno e degli strumenti informatici (*internet* e PC)	2

Processo **Gestione *Privacy***				Giudizio Preliminare [2]	Controlli Esistenti						Valutazione Controlli [3]	Ruolo della Funzione					
Sigla Area/Funz.	N. Fase/Attività	Cod. Reato	Fattore [1]		Esistenza di Procedure	Aggiornamento Procedure	Esistenza di Deleghe	Conoscenza e Comunicazione	Suddivisione Compiti	Controlli e Monitoraggi		Operativo	Decisionale	Autorizzativo	Monitoraggio	Sanzionatorio	*Training*
RU/ DPO/ IT	1	4.1	I, E, D	M	☑	☑	☑	☑	☑	☑	M	☑	☑	☑	☑	☑	☑

Annotazioni. Esiste una prassi supportata da procedura interna (DPS) per la gestione dei dati individuali sensibili e ordinari del personale interno e somministrato e dei dati di Clienti, Fornitori, Soggetti incaricati del controllo, ecc.. L'accesso ai dati individuali dei dipendenti di struttura (es. cedolini) sono visibili al solo responsabile; mentre, per quanto riguarda il sistema gestionale, i dati sono salvaguardati da politiche di gestione (ogni soggetto responsabile accede a dati di propria competenza). Le responsabilità sono formalmente attribuite in linea con l'Organigramma aziendale e i criteri di controllo sono adeguati ma migliorabili nella loro intensità in quanto la prevenzione avviene principalmente con attività di tipo formativo e informativo per i dipendenti di struttura e per le Sedi decentrate.

Processo **Utilizzo Sistema Informativo**	Pr eli	Controlli Esistenti							on e	Ruolo della Funzione							

Sigla Area/Funz.	N. Fase/Attività	Cod. Reato	Fattore [1]															
IT	2	4.1 4.13	I, E	M	☑	☑	☑	☑	☑	☑	M	☑	☑	☑	☑	☑	☑

Annotazioni. Si sottolinea che l'accesso alle informazioni che risiedono sui *server* e sulle banche dati aziendali, ivi inclusi i *client*, è limitato da strumenti di autenticazione (nella fattispecie i dipendenti amministrativi, gli amministratori di sistema, gli addetti alla manutenzione sono muniti di credenziali d'accesso) e che l'accesso alle applicazioni, da parte del personale amministrativo, è garantito da strumenti di autorizzazione. Tutti i *server*, i *desktop* e i *laptop* aziendali sono aggiornati con procedura automatica. La rete di trasmissione dati aziendale è protetta da adeguati strumenti di limitazione degli accessi (*firewall*). Presso la Sede Amministrativa i dispositivi telematici di instradamento sono collocati in aree dedicate e protetti al fine di renderli accessibili al solo personale autorizzato; nelle filiali i dispositivi sono comunque collocati in armadi *rack*. Tutti i dispositivi aziendali sono protetti da programmi *antivirus*, aggiornati in modo automatico, contro il rischio di intrusione. Esistono controlli strutturati e pianificati con procedure e programmi; tuttavia, esiste la variabile delle sedi territoriali che potrebbe determinare lievi e residuali situazioni di difformità e inadempienze.

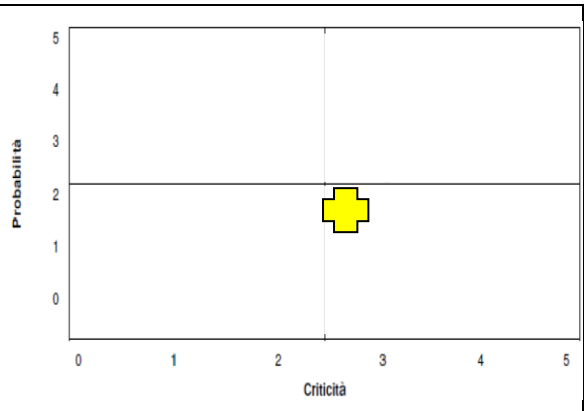
1 I = Interno, E = Esterno, D = Decisionale. **2** Giudizio preliminare rischio reato: A = Alto, M = Medio, B = Basso, I = Inesistente. **3** Valutazione efficacia e adeguatezza dei controlli: I = Inefficaci, M = da migliorare, E = Efficaci, N = Non Esistenti. 4 ☒ = Elemento non presente; ☑ = Elemento Presente.

4.3 – Valutazione del Rischio

Nell'ambito dei singoli rischi di reato, potenzialmente attivi ognuna delle aree aziendali analizzate, se ne valuta la *magnitudo* di ognuno di essi sulla base delle variabili: probabilità e impatto e, sulla base del valore ottenuto e degli scostamenti, si definisce un piano operativo definendo innanzitutto le tipologie di misure preventive e di controllo da attuare.

Casistica 1. Si consideri l'Area RU/DPO/IT nell'ambito del Trattamento dei dati individuali sensibili e ordinari.

Probabilità							
Molto alta	0,45	0,00	2,25	4,50	9,00	18,00	36,00
Alta	0,35	0,00	1,75	3,50	7,00	14,00	28,00
Media	0,25	0,00	1,25	2,50	5,00	10,00	20,00
Bassa	0,15	0,00	0,75	1,50	3,00	6,00	12,00
Molto bassa	0,05	0,00	0,25	0,50	1,00	2,00	4,00
Nulla	0,00	0,00	0,00	0,00	0,00	0,00	0,00
		0	5	10	20	40	80
		Nullo	Molto basso	Basso	Medio	Alto	Molto alto
		Impatto					



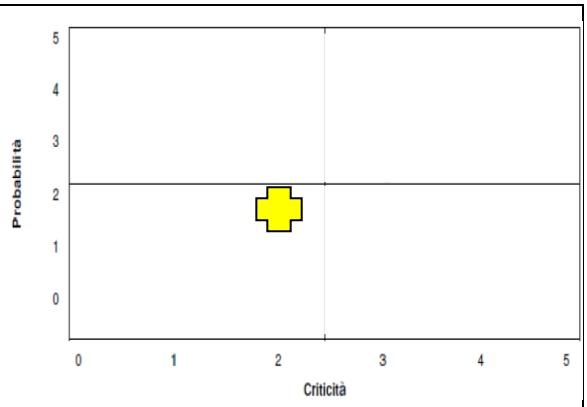
Probabilità	Impatto	Indice di Valutazione:
0,15	**40**	**6**

La Magnitudo si ottiene moltiplicando le variabili P e I (**M = P * I**); da cui ne deriva che l'Esposizione che può essere classificata **Bassa**, **Media** o **Elevata**. Strategie di *risk response*. Per un rischio alto: **evitare** il rischio (*risk avoidance*), per un rischio medio: **limitare** il rischio (*risk reduction*) o **trasferire** il rischio (*risk transferring/sharing*), per il rischio basso: **accettare** il rischio (*risk acceptance*).

Annotazioni sulla valutazione. Si decide di attribuire una magnitudo del rischio media in quanto i controlli sono pianificati, esistenti e operativi, ma il rischio residuo è principalmente dovuto alla necessità di intensificare lo stato dei controlli e all'opportunità di "de-burocratizzare" il sistema di gestione. Per questo la magnitudo attribuita è media e le azioni preventive da adottare devono essere dirette alla più alta e continuativa limitazione del rischio.

Casistica 2. Si consideri l'Area Dipendenti della società nell'ambito dell'Utilizzo del Sistema Informativo, internet e PC.

Probabilità							
Molto alta	0,45	0,00	2,25	4,50	9,00	18,00	36,00
Alta	0,35	0,00	1,75	3,50	7,00	14,00	28,00
Media	0,25	0,00	1,25	2,50	5,00	10,00	20,00
Bassa	0,15	0,00	0,75	1,50	3,00	6,00	12,00
Molto bassa	0,05	0,00	0,25	0,50	1,00	2,00	4,00
Nulla	0,00	0,00	0,00	0,00	0,00	0,00	0,00
		0	5	10	20	40	80
		Nullo	Molto basso	Basso	Medio	Alto	Molto alto
		Impatto					



Probabilità	Impatto	Indice di Valutazione:
0,15	**10**	**1,50**

La Magnitudo si ottiene moltiplicando le variabili P e I (**M = P * I**); da cui ne deriva che l'Esposizione che può essere classificata **Bassa**, **Media** o **Elevata**. Strategie di *risk response*. Per un rischio alto: **evitare** il rischio (*risk avoidance*), per un rischio medio: **limitare** il rischio (*risk reduction*) o **trasferire** il rischio (*risk transferring/sharing*), per il rischio basso: **accettare** il rischio (*risk acceptance*).

Annotazioni sulla valutazione. In relazione alle attività svolte in Sede Amministrativa e presso le Filiali sulle postazioni personali, si decide di attribuire una magnitudo del rischio bassa in quanto i controlli esistenti sono adeguati, effettivamente operativi e commisurati all'entità del rischio; il rischio residuo è comunque rappresentato dal fatto che il personale che opera presso sedi decentrate potrebbe risultare, in casi limite, fuori controllo e potrebbe aggirare i sistemi di controllo fraudolentemente.

La Magnitudo si ottiene moltiplicando le variabili P e I (**M = P * I**); da cui ne deriva che l'Esposizione che può essere classificata **Bassa**, **Media** o **Elevata**. Strategie di *risk response*. Per un rischio alto: **evitare** il rischio (*risk avoidance*), per un rischio medio: **limitare** il rischio (*risk reduction*) o **trasferire** il rischio (*risk transferring/sharing*), per il rischio basso: **accettare** il rischio (*risk acceptance*).

4.4 – Misure e Procedure

Sulla base dei rischi rilevati si stabiliscono le specifiche azioni preventive, le tempistiche, gli strumenti/risorse e le relative responsabilità.

Casistica 1 - Trattamento dei dati individuali sensibili e ordinari

Casistica	Responsabile	Descrizione attività di controllo, risorse, strumenti
1	O.d.V.	Consegnare/esporre/pubblicare il Codice Etico (§§: 4.2.13 Salvaguardia della *privacy*).
1	Risorse Umane	Prevedere periodiche azioni formative/informative verso il personale Sede Amm.va
1	Risorse Umane	Prevedere periodiche azioni formative/informative verso il personale delle Filiali.
1	Risorse Umane	Prevedere specifiche azioni formative/informative verso il personale neoassunto
1	IT	Trasmissione di relazione tecnica sull'efficacia del Sistema di prevenzione e gestione dei dati individuali.
1	O.d.V.	Organizzazione di canali d'informazione tra O.d.V. e parti interessate su casi ritenuti a rischio in applicazione della Procedura PRT 03 - Protocollo segnalazioni di illeciti e irregolarità
1	O.d.V.	L'O.d.V. deve acquisire informazioni in merito all'efficacia delle azioni adottate, eventualmente prescrivere azioni integrative e informare il vertice aziendale.
1	O.d.V.	Redazione di Piano Annuale e consuntivo su Relazione Finale (§ 7 Parte Generale)

Casistica 2 - Utilizzo del Sistema Informativo interno, internet e dei PC

Casistica	Responsabile	Descrizione attività di controllo, risorse, strumenti
2	O.d.V.	Consegnare/esporre/pubblicare il Codice Etico (§§:4.2.12 Utilizzo dei sistemi informatici)
2	IT	Prevedere periodiche azioni formative/informative verso il personale Sede Amm.va
2	IT	Prevedere periodiche azioni formative/informative verso il personale delle Filiali.
2	IT	Prevedere specifiche azioni formative/informative verso il personale neoassunto
2	IT	Trasmissione di relazione tecnica sull'efficacia del Sistema di prevenzione reati informatici.
2	IT	Prevedere che si effettuino controlli (registrati) in remoto e/o in loco sui seguenti *item*: a) il personale deve accedere al sistema informativo aziendale unicamente attraverso i codici di identificazione assegnati, provvedendo alla modifica periodica; b) il personale deve astenersi da qualsiasi condotta (anche colposa) che possa compromettere la riservatezza e integrità delle informazioni e dei dati aziendali interni e di terzi (es. non autorizzati accessi a dati informatici di terzi, intercettazione e diffusione di dati altrui); c) il personale deve astenersi da qualsiasi condotta diretta a superare o aggirare le protezioni del sistema informativo aziendale o altrui; d) il personale deve conservare i codici identificativi assegnati, astenendosi dal comunicarli a terzi che in tal modo potrebbero accedere abusivamente a dati aziendali riservati; e) il personale non può installare programmi senza aver preventivamente informato la funzione aziendale preposta alla gestione della sicurezza informatica; f) il personale non può, forzando il sistema, utilizzare connessioni alternative rispetto a quelle fornite dalla Società nell'espletamento dell'attività lavorativa resa in suo favore. g) il personale non può utilizzare sistemi informatici di archiviazione dati con finalità contrarie alla legge. IT a tal fine predispone idonee Liste di riscontro e redige un verbale a conclusione delle attività di *auditing* che verrà presentato all'O.d.V..
2	O.d.V.	L'O.d.V. deve acquisire informazioni in merito all'efficacia delle azioni adottate, eventualmente prescrivere azioni integrative e informare il vertice aziendale.
2	IT	Messa in opera di nuovi sistemi avanzati di reporting e di sicurezza informatica in Sede e presso le Filiali più grandi.
2	O.d.V.	Redazione di Piano Annuale e consuntivo su Relazione Finale (§ 7 Parte Generale)

CAPITOLO 5: Reati derivanti dall'inosservanza di norme sulla sicurezza e la tutela della salute dei lavoratori

5.1 – Principali riferimenti normativi

Articoli di Legge	Cod.
D.Lgs. D.Lgs. 81/08 - Testo Unico in materia di igiene e sicurezza sul lavoro (Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123 (art. 25 septies), in materia di tutela della salute e della sicurezza nei luoghi di lavoro);	5.1
Decreto Legislativo 3 agosto 2009, n. 106;	
D. Lgs. 123/07 - Misure in tema di tutela della salute dei lavori sui luoghi di lavoro;	5.2
Artt. 589 e 590 c.p.: Omicidio colposo, lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.	5.3

5.2 – Analisi iniziale

Con l'entrata in vigore del D. Lgs. 123/07, si riconosce come fattispecie di reato ai sensi del D. Lgs. 231/01 anche il reato commesso in violazione di norme antinfortunistiche e sulla tutela dell'igiene e salute sul lavoro e in particolare:

- l'omicidio colposo
- le lesioni personali colpose ai sensi degli artt. 589 e 590 del Codice Penale.

L'art 30 del D. Lgs. 81/08 indica alcuni riferimenti per la redazione del modello organizzativo in questione.

Articolo 30 - Modelli di organizzazione e di gestione (estratto)

1. Il modello di organizzazione e di gestione idoneo ad avere efficacia esimente della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica di cui al Decreto Legislativo 8 giugno 2001, n. 231, deve essere adottato ed efficacemente attuato, assicurando un sistema aziendale per l'adempimento di tutti gli obblighi giuridici relativi:
    a) al rispetto degli standard tecnico-strutturali relativi a attrezzature, impianti, luoghi di lavoro;
    b) alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
    c) alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
    d) alle attività di sorveglianza sanitaria;
    e) alle attività di informazione e formazione dei lavoratori;
    f) alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza;
    g) alla acquisizione di documentazioni e certificazioni obbligatorie di legge;
    h) alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.
2. Il modello organizzativo e gestionale di cui al comma 1 deve prevedere idonei sistemi di registrazione dell'avvenuta effettuazione delle attività di cui al comma 1.
3. Il modello organizzativo deve in ogni caso prevedere, per quanto richiesto dalla natura e dimensioni dell'organizzazione e dal tipo di attività svolta, un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.
4. Il modello organizzativo deve altresì prevedere un idoneo sistema di controllo sull'attuazione del medesimo modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del modello organizzativo devono essere adottati, quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico.

La matrice seguente identifica le aree aziendali (funzioni e processi) oggetto di indagine in riferimento ai rischi specifici.

Funzioni/Aree	Processi, fasi e attività	N. casistica
Servizio Prevenzione	Gestione del Servizio di Prevenzione e protezione dai rischi verso personale interno.	1
Servizio Prevenzione	Gestione del Servizio di Prevenzione e protezione dai rischi verso personale somministrato	2

Processo **SPP personale interno**				Giudizio Preliminare [2]	Controlli Esistenti						Valutazione Controlli [3]	Ruolo della Funzione					
Sigla Area/Funz.	N. Fase/Attività	Cod. Reato	Fattore [1]		Esistenza di Procedure	Aggiornamento Procedure	Esistenza di Deleghe	Conoscenza e Comunicazione	Suddivisione Compiti	Controlli e Monitoraggi		Operativo	Decisionale	Autorizzativo	Monitoraggio	Sanzionatorio	*Training*
SPP	1	5	I, E, D	B	☑	☑	☑	☑	☑	☑	E	☑	☑	☑	☑	☑	☑

Annotazioni. Esiste una prassi supportata da procedura interna per la gestione del rischio residuo e per la prevenzione di malattie professionali. Nell'ambito del D.Lgs. 231/01 si considerano unicamente gli artt. Artt. 589 e 590 c.p. omicidio colposo, lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro; in questo ambito, per i lavoratori di Etjca, la valutazione del rischio porta a una valutazione preliminare di basso impatto. In ogni caso le responsabilità sono formalmente attribuite e i criteri di controllo sono adeguati. Sotto la supervisione e il controllo del Responsabile del Servizio di Prevenzione e Protezione (RSPP) tutti i Destinatari a vario titolo coinvolti nella gestione del sistema sicurezza danno attuazione, ciascuno per la parte di propria competenza e nel rispetto delle deleghe e procure attribuite dalla Società nonché delle procedure aziendali vigenti in tale ambito, alle misure di prevenzione e di protezione predisposte a presidio dei rischi connessi alla sicurezza identificati nel Documento di Valutazione dei Rischi ("DVR") che viene periodicamente aggiornato. Tutti i dipendenti interni sono sottoposti a visite mediche periodiche effettuate dal Medico Competente. Ogni comportamento contrario al sistema sicurezza adottato dalla Società viene sanzionato quale violazione del Modello, nell'ambito di un procedimento disciplinare conforme alle previsioni della normativa in materia di rapporti di lavoro. Sono attuate le azioni formative e informative verso i dipendenti.

Processo **SPP personale somministrato**				Giudizio Preliminare [2]	Controlli Esistenti						Valutazione Controlli [3]	Ruolo della Funzione					
Sigla Area/Funz.	N. Fase/Attività	Cod. Reato	Fattore [1]		Esistenza di Procedure	Aggiornamento Procedure	Esistenza di Deleghe	Conoscenza e Comunicazione	Suddivisione Compiti	Controlli e Monitoraggi		Operativo	Decisionale	Autorizzativo	Monitoraggio	Sanzionatorio	*Training*
SPP	2	5	I, E, D	B	☑	☑	☑	☑	☑	☑	E	☑	☑	☑	☑	☑	☑

Annotazioni. L'area di attività ritenuta più specificamente a rischio in relazione ai reati in tema di salute e sicurezza sul lavoro è la gestione della sicurezza e la salute dei lavoratori somministrati. La normativa prevede che il somministratore informi preventivamente i lavoratori sui rischi per la sicurezza e la salute connessi alle attività produttive in generale e che l'impresa utilizzatrice formi e addestri i lavoratori all'utilizzo delle attrezzature di lavoro necessarie allo svolgimento della attività lavorativa per la quale essi vengono assunti e che, previo accordo con il nostro SPP, fornisca loro idonei Dispositivi di protezione Individuale – DPI (art. 23 del D.Lgs. 276/2003, comma 5). L'attuazione delle modalità descritte viene garantita dalle clausole contrattuali previste sia nel contratto di somministrazione che nel contratto di prestazione.

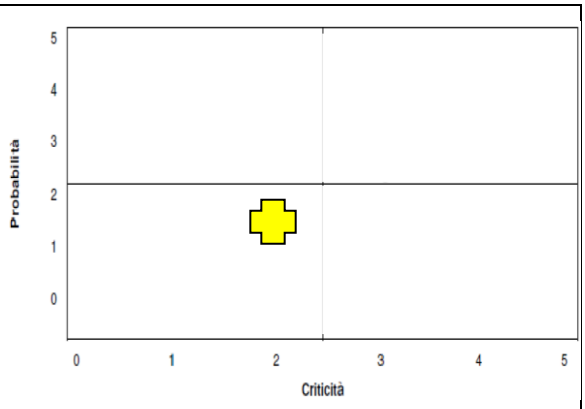
1 I = Interno, E = Esterno, D = Decisionale. **2** Giudizio preliminare rischio reato: A = Alto, M = Medio, B = Basso, I = Inesistente. **3** Valutazione efficacia e adeguatezza dei controlli: I = Inefficaci, M = da migliorare, E = Efficaci, N = Non Esistenti. 4 ☒ = Elemento non presente; ☑ = Elemento Presente..

5.3 – Valutazione del Rischio

Nell'ambito dei singoli rischi di reato, potenzialmente attivi ognuna delle aree aziendali analizzate, se ne valuta la *magnitudo* di ognuno di essi sulla base delle variabili: probabilità e impatto e, sulla base del valore ottenuto e degli scostamenti, si definisce un piano operativo definendo innanzitutto le tipologie di misure preventive e di controllo da attuare .

Casistica 1. Si consideri l'Area del Servizio di Prevenzione e Protezione verso personale interno.

Probabilità							
Molto alta	0,45	0,00	2,25	4,50	9,00	18,00	36,00
Alta	0,35	0,00	1,75	3,50	7,00	14,00	28,00
Media	0,25	0,00	1,25	2,50	5,00	10,00	20,00
Bassa	0,15	0,00	0,75	1,50	3,00	6,00	12,00
Molto bassa	0,05	0,00	0,25	0,50	1,00	2,00	4,00
Nulla	0,00	0,00	0,00	0,00	0,00	0,00	0,00
		0	5	10	20	40	80
		Nullo	Molto basso	Basso	Medio	Alto	Molto alto
		Impatto					



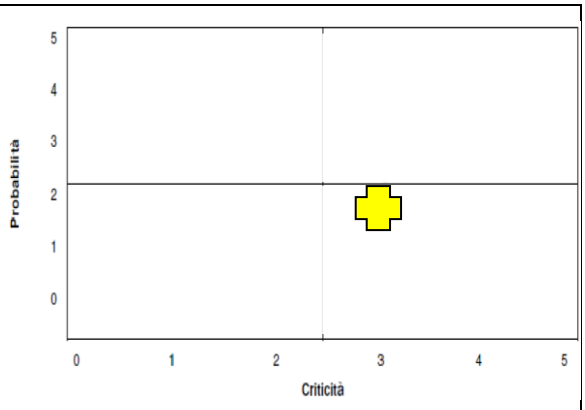
Probabilità	Impatto	Indice di Valutazione:
0,05	**10**	**0,50**

La Magnitudo si ottiene moltiplicando le variabili P e I (**M = P * I**); da cui ne deriva che l'Esposizione che può essere classificata **Bassa**, **Media** o **Elevata**. Strategie di *risk response*. Per un rischio alto: **evitare** il rischio (*risk avoidance*), per un rischio medio: **limitare** il rischio (*risk reduction*) o **trasferire** il rischio (*risk transferring/sharing*), per il rischio basso: **accettare** il rischio (*risk acceptance*).

Annotazioni sulla valutazione. Si decide di attribuire una magnitudo del rischio bassa in quanto i controlli per il personale interno sono esistenti e operativi. Pertanto, il vigente sistema di controlli è adeguato e idoneo. Sarà comunque necessario attuare controlli preventivi seguendo scrupolosamente le indicazioni impartite dal Responsabile del Servizio Prevenzione e Protezione.

Casistica 2. Si consideri l'Area del Servizio di Prevenzione e Protezione verso personale somministrato.

Probabilità							
Molto alta	0,45	0,00	2,25	4,50	9,00	18,00	36,00
Alta	0,35	0,00	1,75	3,50	7,00	14,00	28,00
Media	0,25	0,00	1,25	2,50	5,00	10,00	20,00
Bassa	0,15	0,00	0,75	1,50	3,00	6,00	12,00
Molto bassa	0,05	0,00	0,25	0,50	1,00	2,00	4,00
Nulla	0,00	0,00	0,00	0,00	0,00	0,00	0,00
		0	5	10	20	40	80
		Nullo	Molto basso	Basso	Medio	Alto	Molto alto
		Impatto					



Probabilità	Impatto	Indice di Valutazione:
0,15	**20**	**3**

La Magnitudo si ottiene moltiplicando le variabili P e I (**M = P * I**); da cui ne deriva che l'Esposizione che può essere classificata **Bassa**, **Media** o **Elevata**. Strategie di *risk response*. Per un rischio alto: **evitare** il rischio (*risk avoidance*), per un rischio medio: **limitare** il rischio (*risk reduction*) o **trasferire** il rischio (*risk transferring/sharing*), per il rischio basso: **accettare** il rischio (*risk acceptance*).

Annotazioni sulla valutazione. Si decide di attribuire una magnitudo del rischio bassa in quanto la legge e la giurisprudenza prevedono a nostro carico obblighi di tipo amministrativo/contrattuale e obblighi formativi e informativi propedeutici al lavoro, trasferendo alle imprese l'attuazione delle specifiche misure preventive e protettive. In considerazione dei potenziali rischi di cui agli artt. 589 e 590 c.p., devono essere attuati controlli di tipo documentale sui contratti sottoscritti con le imprese e controlli sull'efficacia delle azioni informative verso i dipendenti. L'O.d.V., eventualmente incaricando *auditor* interni, deve vigilare affinché tali controlli siano effettivamente attuati e risultino efficaci.

5.4 – Misure e Procedure

Sulla base dei rischi rilevati si stabiliscono le specifiche azioni preventive, le tempistiche, gli strumenti/risorse e le relative responsabilità.

Casistica	Responsabile	Descrizione attività di controllo, risorse, strumenti
1, 2	O.d.V.	Consegnare/esporre/pubblicare il Codice Etico
1	RSPP	Prevedere specifiche azioni informative verso il personale interno neoassunto
2	RSPP	Prevedere specifiche azioni formative/informative verso il personale somministrato
2	Risorse Umane	Prevedere manleva per consegna DPI e acquisizione di informazioni preliminari alla stipula del contratto con l'impresa utilizzatrice.
2	RSPP	Prevedere azioni specifiche di controllo programmate, strutturate e pianificate (almeno annuali) su: - Compilazione allegato 1 al Contratto con le Imprese utilizzatrici; - Attuazione dei programmi formativi e informativi per il personale. RSPP redige un verbale a conclusione delle attività di *auditing* che verrà presentato almeno all'O.d.V..
1,2	RSPP	Trasmette periodicamente dati e informazioni utili all'O.d.V. riconducibili al controllo operativo del SPP.
1, 2	O.d.V.	Organizzazione di canali d'informazione tra O.d.V. e parti interessate su casi ritenuti a rischio in applicazione della Procedura PRT 03 - Protocollo segnalazioni di illeciti e irregolarità
1, 2	O.d.V.	L'O.d.V. verifica l'efficacia delle azioni adottate, eventualmente prescrivere azioni integrative e informa il vertice aziendale.
1, 2	O.d.V.	L'O.d.V. documenta in forma scritta i controlli effettuati e i risultati ottenuti mediante consuntivo specifico sul Piano Annuale e relazione Finale

CAPITOLO 6: Reati da violazione del diritto d'autore

6.1 – Principali riferimenti normativi

Articoli di Legge	Cod.
art. 171 comma 1 lettera a – bis) e c), che punisce chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma, mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essi, ovvero compie i fatti indicati nelle precedenti lettere mediante una delle forme di elaborazione previste da questa legge.	6.1
art. 171-bis, che punisce chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE), anche se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori, ovvero chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati ovvero esegue l'estrazione o il reimpiego della banca di dati, ovvero distribuisce, vende o concede in locazione una banca di dati.	6.2
art. 171-ter, che punisce chiunque a fini di lucro, se il fatto è commesso per uso non personale: a) abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; b) abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico/musicali, ovvero multimediali, anche se Parte Speciale – Industria Commercio Diritti d'Autore 6 inserite in opere collettive o composite o banche dati; ecc. art. 171-septies, che punisce: a) i produttori o importatori dei supporti non soggetti al contrassegno di cui all'articolo 181-bis, i quali non comunicano alla SIAE entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione i dati necessari alla univoca identificazione dei supporti medesimi; b) chiunque dichiari falsamente l'avvenuto assolvimento degli obblighi di cui all'articolo 181-bis, comma 2, della presente legge.	6.3
art. 171-octies, che punisce chiunque a fini fraudolenti produce, pone in vendita, importa, promuove, installa, modifica, utilizza per uso pubblico e privato 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. Si intendono ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti italiane o estere in forma tale da rendere gli stessi visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dalla imposizione di un canone per la fruizione.	6.4
Legge n. 238/2021; Regolamento (UE) n. 1031/2010 della Commissione, del 12 novembre 2010	6.5

6.2 – Analisi iniziale

La matrice seguente identifica le aree aziendali (funzioni e processi) oggetto di indagine in riferimento ai rischi specifici.

Funzioni/Aree	Processi, fasi e attività	N. casistica
Responsabile dei Sistemi Informativi	Utilizzo del Sistema Informativo interno, internet e dei PC	1

Processo **Utilizzo Sistema Informativo**				Giudizio Preliminare [2]	Controlli Esistenti						Valutazione Controlli [3]	Ruolo della Funzione					
Sigla Area/Funz.	N. Fase/Attività	Cod. Reato	Fattore [1]		Esistenza di Procedure	Aggiornamento Procedure	Esistenza di Deleghe	Conoscenza e Comunicazione	Suddivisione Compiti	Controlli e Monitoraggi		Operativo	Decisionale	Autorizzativo	Monitoraggio	Sanzionatorio	*Training*
IT	1	6.1 6.2 6.4	I, E	I	☒	☒	☒	☒	☒	☒	N	☒	☒	☒	☒	☒	☒
IT	1	6.3	I, E	B	☑	☑	☑	☑	☑	☑	E	☑	☑	☑	☑	☑	☑

1 I = Interno, E = Esterno, D = Decisionale. **2** Giudizio preliminare rischio reato: A = Alto, M = Medio, B = Basso, I = Inesistente. **3** Valutazione efficacia e adeguatezza dei controlli: I = Inefficaci, M = da migliorare, E = Efficaci, N = Non Esistenti. 4 ☒ = Elemento non presente; ☑ = Elemento Presente..

La Legge n. 238/2021, pubblicata in Gazzetta Ufficiale lo scorso 17 gennaio ed entrata in vigore il 1° febbraio 2022, in un'ottica di uniformazione delle previsioni di diritto nazionale alle richieste del diritto europeo, è intervenuta apportando significative modifiche ad alcune fattispecie del Codice penale, rientranti nell'ambito dei reati presupposto di cui al D.Lgs. 231/2001. Nello specifico l'articolo 26 della legge 238/2021 introduce alcune modifiche ad alcuni reati richiamati dall'art. 25 sexies del D.Lgs. 231/2001 "Reati di abuso di mercato". In particolare, l'articolo 184 T.U.F. ora rubricato "Abuso o comunicazione illecita di informazioni privilegiate" prevede:

- un inasprimento delle pene per i c.d. *insider* primari e per i c.d. *criminal insider*: la pena della reclusione viene innalzata fino a due anni nel minimo e dodici anni nel massimo, unitamente alla previsione di una multa da 20.000 euro a 3 milioni di euro;
- la definitiva introduzione della punibilità dell'insider secondario con la previsione della pena della reclusione da un anno e sei mesi fino a dieci anni e la multa da 20.000 euro a 2,5 milioni di euro, salvi i casi di concorso con gli insider primari in cui si applicheranno le sanzioni loro riferite e l'estensione dell'aggravante ex 184, comma 3, T.U.F. viene estesa allo stesso insider secondario
- un aumento di pena della multa fino al triplo o fino al maggior importo di dieci volte il prodotto o il profitto conseguito dal reato quando, per la rilevante offensività del fatto, per le qualità personali del colpevole o per l'entità del prodotto o del profitto conseguito dal reato, essa appare inadeguata anche se applicata nel massimo;
- l'applicazione delle disposizioni dell'articolo anche ai fatti che riguardano condotte od operazioni, comprese le offerte, relative alle aste su una piattaforma d'asta autorizzata, come un mercato regolamentato di quote di emissioni o di altri prodotti oggetto d'asta correlati, anche quando i prodotti oggetto d'asta non sono strumenti finanziari, ai sensi del regolamento (UE) n. 1031/2010 della Commissione, del 12 novembre 2010.

Da notare che l'ambito di applicazione della confisca obbligatoria viene ora limitato al solo profitto del reato di abuso o comunicazione illecita di informazioni privilegiate o manipolazione di mercato e non anche ai mezzi usati per commettere il reato.

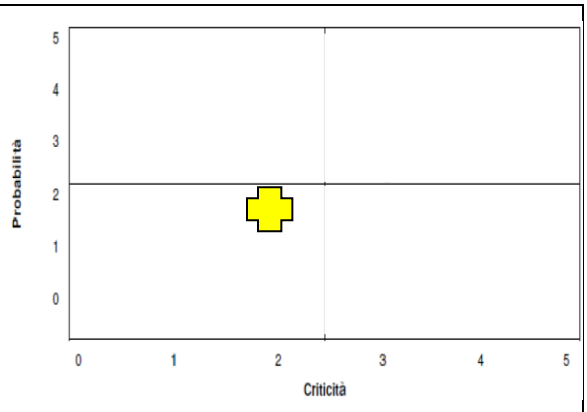
Annotazioni. Si consideri praticamente nullo il rischio legato all'abusiva commercializzazione di prodotti, dispositivi e beni immateriali protetti dal diritto d'autore; l'unica residuale problematica che potrebbe verificarsi presso le sedi è il *file sharing (download file)* (rif. Cod. reato: 6.3) di materiale informatico/pubblicazioni/audio/video protetti dalle leggi sul diritto d'autore (ex art. 171-ter, lett. a, b); pur escludendo, presso la nostra organizzazione, un elevato rischio del manifestarsi del fenomeno della vendita/commercializzazione abusiva, tuttavia le procedure interne dovrebbero portare alla prevenzione di casi isolati commessi da dipendenti di struttura (soprattutto quelli che lavorano presso le Sede decentrate). Si sottolinea tuttavia che il traffico sulla rete dati è comunque filtrato al fine di prevenire l'utilizzo di programmi di *file sharing*.

6.3 – Valutazione del Rischio

Nell'ambito dei singoli rischi di reato, potenzialmente attivi ognuna delle aree aziendali analizzate, se ne valuta la *magnitudo* di ognuno di essi sulla base delle variabili: probabilità e impatto e, sulla base del valore ottenuto e degli scostamenti, si definisce un piano operativo definendo innanzitutto le tipologie di misure preventive e di controllo da attuare.

Casistica 1. Si consideri l'Area IT nell'ambito Utilizzo del Sistema Informativo interno, internet e dei PC.

Probabilità							
Molto alta	0,45	0,00	2,25	4,50	9,00	18,00	36,00
Alta	0,35	0,00	1,75	3,50	7,00	14,00	28,00
Media	0,25	0,00	1,25	2,50	5,00	10,00	20,00
Bassa	0,15	0,00	0,75	1,50	3,00	6,00	12,00
Molto bassa	0,05	0,00	0,25	0,50	1,00	2,00	4,00
Nulla	0,00	0,00	0,00	0,00	0,00	0,00	0,00
		0	5	10	20	40	80
		Nullo	Molto basso	Basso	Medio	Alto	Molto alto
		Impatto					



Probabilità	Impatto	Indice di Valutazione:
0,15	**10**	**1,5**

La Magnitudo si ottiene moltiplicando le variabili P e I (**M = P * I**); da cui ne deriva che l'Esposizione che può essere classificata **Bassa**, **Media** o **Elevata**. Strategie di *risk response*. Per un rischio alto: **evitare** il rischio (*risk avoidance*), per un rischio medio: **limitare** il rischio (*risk reduction*) o **trasferire** il rischio (*risk transferring/sharing*), per il rischio basso: **accettare** il rischio (*risk acceptance*).

Annotazioni sulla valutazione. Si decide di attribuire una magnitudo del rischio bassa in quanto i controlli sono esistenti, operativi ed efficaci; esiste tuttavia un rischio residuo da tenere sotto controllo. Sulla scorta di quanto già scritto a proposito dei reati informatici (ved. § 4) sarà opportuno pianificare, strutturare e attuare controlli preventivi a cura del Responsabile dei Sistemi Informativi.

6.4 – Misure e Procedure

Sulla base dei rischi rilevati si stabiliscono le specifiche azioni preventive, le tempistiche, gli strumenti/risorse e le relative responsabilità.

Casistica	Responsabile	Descrizione attività di controllo, risorse, strumenti
1	O.d.V.	Consegnare/esporre/pubblicare il Codice Etico
1	IT	Formazione/informazione specifica per il personale
1	IT	Trasmissione di relazione tecnica sull'efficacia del Sistema di prevenzione reati in violazione del diritto d'autore.
1	IT	Prevedere che si effettuino controlli (registrati) in remoto o in loco sui seguenti *item*: a) il personale deve astenersi dall'utilizzare strumenti informatici aziendali per scaricare materiali protetti da *copy right*; b) il personale deve astenersi da qualsiasi condotta diretta a superare o aggirare le protezioni del sistema informativo aziendale o altrui; c) il personale non può installare programmi senza aver preventivamente informato la funzione aziendale preposta alla gestione della sicurezza informatica; d) il personale non può utilizzare connessioni alternative rispetto a quelle fornite dalla Società nell'espletamento dell'attività lavorativa resa in suo favore; e) il personale non può utilizzare sistemi informatici di archiviazione dati con finalità contrarie alla legge. IT a tal fine predispone idonee Liste di riscontro e redige un verbale a conclusione delle attività di *auditing* che verrà presentato all'O.d.V..
1	O.d.V.	L'O.d.V. deve acquisire informazioni in merito all'efficacia delle azioni adottate, eventualmente prescrivere azioni integrative e informare il vertice aziendale.
1	IT	Messa in opera di nuovi sistemi avanzati di reporting e di sicurezza informatica in Sede e presso le Filiali più grandi.
1	O.d.V.	Redazione di Piano Annuale e consuntivo su Relazione Finale (§ 7 Parte Generale)

CAPITOLO 7: Reati contro la personalità Individuale

7.1 – Principali riferimenti normativi

Articoli di Legge	Cod.
art. 600 c.p. Riduzione o mantenimento in schiavitù o in servitù	7.1
art. 600 *bis* c.p. Prostituzione minorile	7.2
art. 600 *ter* c.p. Pornografia minorile	7.3
art. 600 *quater* c.p. Detenzione di materiale pedo-pornografico	7.4
art. 600 *quater* c.p. - Pornografia virtuale	7.5
art. 601 c.p. Tratta di persone	7.6
art. 602 c.p. Acquisto e alienazione di schiavi	7.7
art. 583-*bis* c.p. Pratiche di mutilazione degli organi genitali femminili	7.8
D.Lgs. N. 74 del 12/05/2016 - Disposizioni in materia di certificazione casellario giudiziale del lavoratore	7.9
DPR 14/11/2002 N. 313	7.10
Legge n. 238/2021	7.11
Direttiva n. 2011/93/UE	7.12

7.2 – Analisi iniziale

La matrice seguente identifica le aree aziendali (funzioni e processi) oggetto di indagine in riferimento ai rischi specifici.

Funzioni/Aree	Processi, fasi e attività	Casistica
Responsabile dei Sistemi Informativi	Utilizzo del Sistema Informativo interno, internet e dei PC	1
Ufficio Risorse Umane	Assunzione di lavoratori somministrati nell'ambito di attività che prevedono continuativi rapporti interpersonali con i minori	2

Processo **Utilizzo Sistema Informativo**				Giudizio Preliminare [2]	Controlli Esistenti						Valutazione Controlli [3]	Ruolo della Funzione					
Sigla Area/Funz.	N. Fase/Attività	Cod. Reato	Fattore [1]		Esistenza di Procedure	Aggiornamento Procedure	Esistenza di Deleghe	Conoscenza e Comunicazione	Suddivisione Compiti	Controlli e Monitoraggi		Operativo	Decisionale	Autorizzativo	Monitoraggio	Sanzionatorio	*Training*
IT	1	7.1 7.2 7.6 7.7 7.8	I, E	I	☒	☒	☒	☒	☒	☒	N	☒	☒	☒	☒	☒	☒
IT	1	7.3 7.4 7.5	I, E	B	☑	☑	☑	☑	☑	☑	A	☑	☑	☑	☑	☑	☑

1 I = Interno, E = Esterno, D = Decisionale. **2** Giudizio preliminare rischio reato: A = Alto, M = Medio, B = Basso, I = Inesistente. **3** Valutazione efficacia e adeguatezza dei controlli: I = Inefficaci, M = da migliorare, E = Efficaci, N = Non Esistenti. 4 ☒ = Elemento non presente; ☑ = Elemento Presente.

Annotazioni. Si considerino praticamente nulli rischi di reati commessi contro la personalità individuale; l'unica eccezione è rappresentata dai reati di cui ai §§ 7.3 - 7.5 (vale a dire i reati ex 600 ter c.p. - pornografia minorile e ex art. 600 *quater* c.p. - detenzione di materiale pedo-pornografico e pornografia virtuale). Poiché non è permesso acquisire informazioni sul dipendente (assunto o neoassunto) sulla sua vita privata e su eventuali procedimenti penali a suo carico, risulta allora necessario considerare il rischio legato alla pratica pedo-pornografica sicuramente come caso eccezionale e residuale ma non totalmente improbabile. Esistono procedure interne e strumenti di controllo che dovrebbero portare alla prevenzione di casi isolati che potrebbero essere commessi da dipendenti di struttura (soprattutto da coloro che lavorano presso le Filiali); i controlli non devono comunque essere in contrasto con le vigenti normative giuslavoristiche che garantiscono la *privacy* del dipendente.

Fa eccezione a questa regola di tutela della *privacy* del lavoratore l'assumere informazioni preliminari all'assunzione di persone da impiegare in attività che prevedono continuativi rapporti interpersonali con soggetti minori.

Più recentemente l'articolo 20 della L. 238/2021 modifica i "Delitti contro la personalità individuale", richiamati dall'articolo 25- quinquies del D.Lgs. 231/2001. Nello specifico:

- la rubrica dell'articolo 600-quater è sostituita dalla seguente "Detenzione o accesso a materiale pornografico ed è stata aggiunto il seguente secondo comma: "fuori dei casi di cui al primo comma, chiunque, mediante l'utilizzo della rete internet o di altre reti o mezzi di comunicazione, accede intenzionalmente e senza giustificato motivo a materiale pornografico realizzato utilizzando minori degli anni diciotto è punito con la reclusione fino a due anni e con la multa non inferiore a euro 1.000";
- all'articolo 609-undecies, rubricato "Adescamento di minorenni", viene aggiunto un ulteriore comma che prevede l'aumento di pena in relazione ai seguenti casi: (i) "se il reato è commesso da più persone riunite"; (ii) "se il reato è commesso da una persona che fa parte di una associazione per delinquere al fine di agevolarne l'attività"; (iii) "se dal fatto, a causa della reiterazione delle condotte, deriva al minore un pregiudizio grave"; e (iv) "se dal fatto deriva pericolo di vita per il minore".

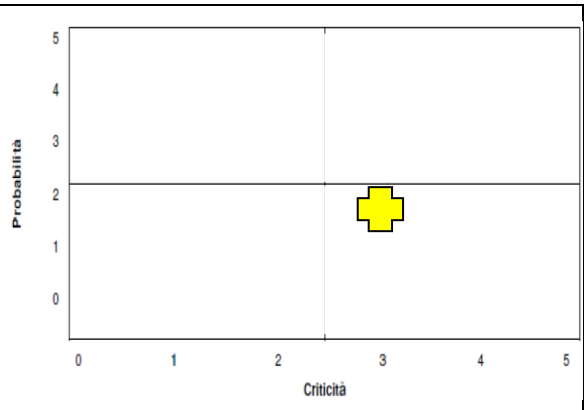
Da ultimo la Legge n. 238/2021, pubblicata in Gazzetta Ufficiale lo scorso 17 gennaio ed entrata in vigore il 1° febbraio 2022, in un'ottica di uniformazione delle previsioni di diritto nazionale alle richieste del diritto europeo, è intervenuta apportando significative modifiche ad alcune fattispecie del Codice penale, rientranti nell'alveo dei reati presupposto di cui al D.Lgs. 231/2001. Nello specifico, le linee di intervento possono essere identificate nell'adeguamento adeguamento alla Direttiva n. 2011/93/UE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile – modifica degli artt. 600-quater e 609-undecies c.p., presupposto della responsabilità degli enti

7.3 – Valutazione del Rischio

Nell'ambito dei singoli rischi di reato, potenzialmente attivi ognuna delle aree aziendali analizzate, se ne valuta la *magnitudo* di ognuno di essi sulla base delle variabili: probabilità e impatto e, sulla base del valore ottenuto e degli scostamenti, si definisce un piano operativo definendo innanzitutto le tipologie di misure preventive e di controllo da attuare.

Casistica 1. Si consideri l'Area IT nell'ambito Utilizzo del Sistema Informativo interno, internet e dei PC.

Probabilità							
Molto alta	0,45	0,00	2,25	4,50	9,00	18,00	36,00
Alta	0,35	0,00	1,75	3,50	7,00	14,00	28,00
Media	0,25	0,00	1,25	2,50	5,00	10,00	20,00
Bassa	0,15	0,00	0,75	1,50	3,00	[illegible]	12,00
Molto bassa	0,05	0,00	0,25	0,50	1,00	2,00	4,00
Nulla	0,00	0,00	0,00	0,00	0,00	0,00	0,00
		0	5	10	20	40	80
		Nullo	Molto basso	Basso	Medio	Alto	Molto alto
		Impatto					



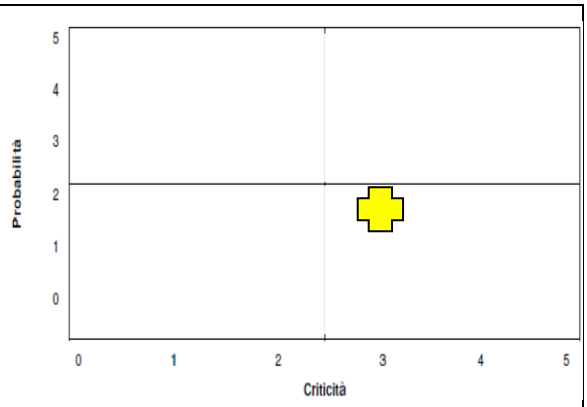
Probabilità	Impatto	Indice di Valutazione:
0,05	**40**	**2**

La Magnitudo si ottiene moltiplicando le variabili P e I (**M = P * I**); da cui ne deriva che l'Esposizione che può essere classificata **Bassa**, **Media** o **Elevata**. Strategie di *risk response*. Per un rischio alto: **evitare** il rischio (*risk avoidance*), per un rischio medio: **limitare** il rischio (*risk reduction*) o **trasferire** il rischio (*risk transferring/sharing*), per il rischio basso: **accettare** il rischio (*risk acceptance*).

Annotazioni sulla valutazione. Nonostante l'elevato impatto, si decide di attribuire una *magnitudo* del rischio bassa in quanto i controlli sono esistenti, operativi ed efficaci, ma esiste tuttavia un rischio residuo da tenere sotto controllo in quanto, sebbene esistano procedure e strumenti, esiste personale che opera presso sedi decentrate (che, come tali, possono risultare controllate sporadicamente). Sulla scorta di quanto già scritto a proposito dei reati informatici (ved. § 4) e dei reati da violazione del diritto d'autore (ved. § 6) sarà opportuno pianificare, strutturare e attuare controlli preventivi a cura del Responsabile dei Sistemi Informativi.

Casistica 2. Si consideri l'Area Risorse Umane nell'ambito di assunzioni di personale destinato ad attività continuative con soggetti minori

Probabilità							
Molto alta	0,45	0,00	2,25	4,50	9,00	18,00	36,00
Alta	0,35	0,00	1,75	3,50	7,00	14,00	28,00
Media	0,25	0,00	1,25	2,50	5,00	10,00	20,00
Bassa	0,15	0,00	0,75	1,50	3,00	6,00	12,00
Molto bassa	0,05	0,00	0,25	0,50	1,00	2,00	4,00
Nulla	0,00	0,00	0,00	0,00	0,00	0,00	0,00
		0	5	10	20	40	80
		Nullo	Molto basso	Basso	Medio	Alto	Molto alto
		Impatto					



Probabilità	Impatto	Indice di Valutazione:
0,05	**40**	**2**

La Magnitudo si ottiene moltiplicando le variabili P e I (**M = P * I**); da cui ne deriva che l'Esposizione che può essere classificata **Bassa**, **Media** o **Elevata**. Strategie di *risk response*. Per un rischio alto: **evitare** il rischio (*risk avoidance*), per un rischio medio: **limitare** il rischio (*risk reduction*) o **trasferire** il rischio (*risk transferring/sharing*), per il rischio basso: **accettare** il rischio (*risk acceptance*).

Annotazioni sulla valutazione. Ferma restante la responsabilità dell'utilizzatore delle azioni della manodopera somministrata, esistono tuttavia controlli preliminari all'assunzione volti ad acquisire informazioni nel rispetto della *privacy* del lavoratore destinato a essere impiegato in attività lavorative che comportino un continuativo rapporto con soggetti minori (es.: addetti alle mense scolastiche, insegnanti di scuola materna, autisti di *pullman*, infermieri di reparti pediatriatici, ecc.).

In questi casi Etjca effettua controlli preliminari all'assunzione conformemente al D.Lgs. N. 74 del 12/05/2016; in particolare, prima dell'assunzione, l'Ufficio Risorse Umane richiede agli uffici prepositi il Certificato relativo al casellario giudiziale e, per i casi di rapporti di lavoro più duraturi, il Certificato relativo ai carichi pendenti.

Per i casi più urgenti, qualora l'assunzione dovesse completarsi in tempi inferiori a quelli previsti per l'ottenimento del certificato, viene richiesto al lavoratore una Dichiarazione sostitutiva di non avere carichi pendenti o situazioni passate in giudicato.

Resta fermo il diritto del datore di lavoro (Etjca S.p.A.) di interrompere il rapporto di lavoro qualora, nei periodi successivi alla assunzione, il lavoratore perdesse i requisiti morali, condizione necessaria per la prosecuzione del rapporto di lavoro.

7.4 – Misure e Procedure

Sulla base dei rischi rilevati si stabiliscono le specifiche azioni preventive, le tempistiche, gli strumenti/risorse e le relative responsabilità.

Casistica	Responsabile	Descrizione attività di controllo, risorse, strumenti
1, 2	O.d.V.	Consegnare/esporre/pubblicare il Codice Etico
1, 2	IT / UFF. RU	Formazione/informazione specifica per il personale
1, 2	IT / UFF. RU	Trasmissione di relazione tecnica sull'efficacia del Sistema di prevenzione reati contro la personalità individuale.
1	IT	Prevedere che si effettuino controlli (registrati) in remoto o in loco sui seguenti *item*: a) il personale deve astenersi dall'utilizzare strumenti informatici aziendali e connessioni per scaricare o acquistare materiali lesivi della dignità e integrità della personalità individuale (specie se minorenne); b) il personale deve astenersi dall'utilizzare strumenti informatici aziendali per condividere o commercializzare materiali lesivi della dignità e integrità della personalità individuale (specie se minorenne); c) il personale non può, forzando il sistema, utilizzare connessioni alternative rispetto a quelle fornite dalla Società nell'espletamento dell'attività lavorativa resa in suo favore; d) il personale non può utilizzare sistemi informatici di archiviazione dati con finalità contrarie alla legge. IT a tal fine predispone idonee Liste di riscontro e redige un verbale a conclusione delle attività di *auditing* che verrà presentato all'O.d.V..

2	UFF. RU	Conservare la documentazione specifica del dipendente, es.: Certificazione del Casellario Giudiziale e/o Certificato Carichi Pendenti per una durata non inferiore e non superiore a 10 anni (periodo in cui un eventuale reato cadrebbe in prescrizione).
1, 2	O.d.V.	Organizzazione di canali d'informazione tra O.d.V. e parti interessate su casi ritenuti a rischio in applicazione della Procedura PRT 03 - Protocollo segnalazioni di illeciti e irregolarità
1, 2	O.d.V.	L'O.d.V. deve acquisire informazioni in merito all'efficacia delle azioni adottate, eventualmente prescrivere azioni integrative e informare il vertice aziendale.
1, 2	O.d.V.	Redazione di Piano Annuale e consuntivo su Relazione Finale (§ 7 Parte Generale)

CAPITOLO 8: Reati contro l'Industria e il Commercio

8.1 – Principali riferimenti normativi

Articoli di Legge	Cod.
art. 513 c.p. Turbata libertà dell'industria o del commercio.	8.1
art. 515 c.p. Frode nell'esercizio del commercio.	8.2
art. 516 c.p. Vendita di sostanze alimentari non genuine come genuine.	8.3
art. 517 c.p. Vendita di prodotti industriali con segni mendaci.	8.4
art. 517 *ter* c.p. Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale.	8.5
art. 517 *quater* c.p. Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari.	8.6
art. 513 *bis* c.p. Illecita concorrenza con minaccia o violenza.	8.7
art. 514 c.p. Frodi contro le industrie nazionali.	8.8

8.2 – Analisi iniziale

La matrice seguente identifica le aree aziendali (funzioni e processi) oggetto di indagine in riferimento ai rischi specifici.

Funzioni/Aree	Processi, fasi e attività	Casistica
Nessuna	Nessun processo	/

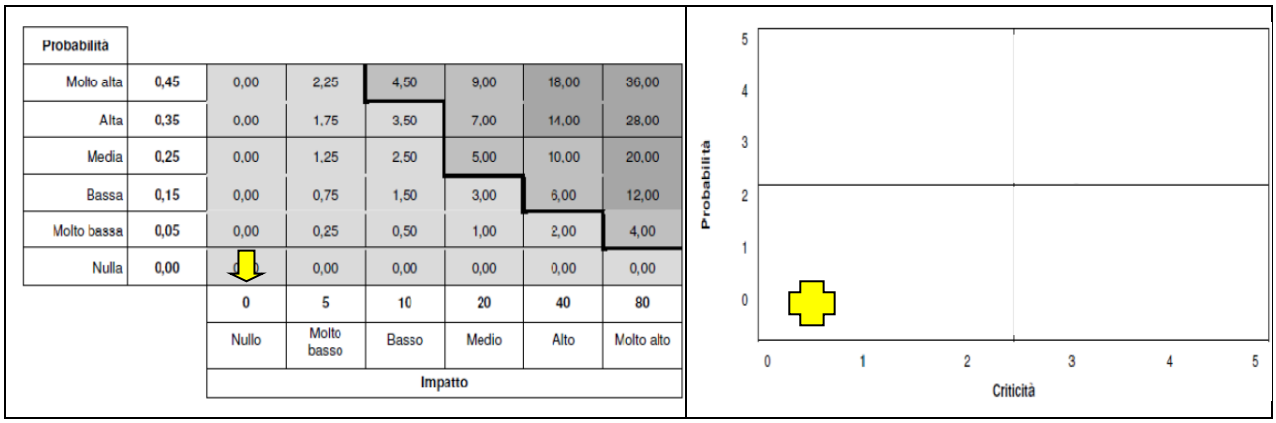
Processo /				Giudizio Preliminare [2]	Controlli Esistenti						Valutazione Controlli [3]	Ruolo della Funzione					
Sigla Area/Funz.	N. Fase/Attività	Cod. Reato	Fattore [1]		Esistenza di Procedure	Aggiornamento Procedure	Esistenza di Deleghe	Conoscenza e Comunicazione	Suddivisione Compiti	Controlli e Monitoraggi		Operativo	Decisionale	Autorizzativo	Monitoraggio	Sanzionatorio	*Training*
/	/	8	I	I	☒	☒	☒	☒	☒	☒	N	☒	☒	☒	☒	☒	☒

1 I = Interno, E = Esterno, D = Decisionale. **2** Giudizio preliminare rischio reato: A = Alto, M = Medio, B = Basso, I = Inesistente. **3** Valutazione efficacia e adeguatezza dei controlli: I = Inefficaci, M = da migliorare, E = Efficaci, N = Non Esistenti. 4 ☒ = Elemento non presente; ☑ = Elemento Presente.

Annotazioni. Si considerino praticamente nulli rischi di reati commessi contro l'Industria e Il Commercio in quanto i servizi erogati da Etjca S.p.A. non contemplano attività che possano ricondurre a frodi nell'esercizio del commercio, contraffazioni di marchi, ecc. Non esistono estremi per rilevare rischi residui e di conseguenza non esistono procedure e controlli specifici.

8.3 – Valutazione del Rischio

Nell'ambito dei singoli rischi di reato, potenzialmente attivi ognuna delle aree aziendali analizzate, se ne valuta la *magnitudo* di ognuno di essi sulla base delle variabili: probabilità e impatto e, sulla base del valore ottenuto e degli scostamenti, si definisce un piano operativo definendo innanzitutto le tipologie di misure preventive e di controllo da attuare.



Probabilità	Impatto	Indice di Valutazione:
0	**0**	**0**

La Magnitudo si ottiene moltiplicando le variabili P e I (**M = P * I**); da cui ne deriva che l'Esposizione che può essere classificata **Bassa**, **Media** o **Elevata**.

Strategie di *risk response*. Per un rischio alto: **evitare** il rischio (*risk avoidance*), per un rischio medio: **limitare** il rischio (*risk reduction*) o **trasferire** il rischio (*risk transferring/sharing*), per il rischio basso: **accettare** il rischio (*risk acceptance*).

Annotazioni sulla valutazione. Non esistono processi a rischio e, di conseguenza, non si attivano controlli specifici.

8.4 – Misure e Procedure

Sulla base dei rischi rilevati si decide di non approvare specifiche azioni preventive.

Casistica	Responsabile	Descrizione attività di controllo, risorse, strumenti
/	/	/

CAPITOLO 9: Falsità in monete, carte di credito, valori di bollo

9.1 – Principali riferimenti normativi

Articoli di Legge	Cod.
art. 453 c.p. Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate.	9.1
art. 454 c.p. Alterazione di monete.	9.2
art. 455 c.p. Spendita e introduzione nello Stato, senza concerto, di monete falsificate.	9.3
art. 457 c.p. Spendita di monete falsificate ricevute in buona fede.	9.4
art. 458 c.p. Parificazione delle carte di pubblico credito alle monete.	9.5
art. 459 c.p. Falsificazione dei valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati.	9.6
art. 460 c.p. Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo.	9.7
art. 461 c.p. Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata.	9.8
art. 464 c.p. Uso di valori di bollo contraffatti o alterati.	9.9
art. 473 c.p. Contraffazione, alterazione o uso di segni distintivi di opere dell'ingegno o di prodotti industriali.	9.10
art. 474 c.p. Introduzione nello Stato e commercio di prodotti con segni falsi.	9.11
art. 493 ter, 493 quater, 640 ter. c.p. Attuazione della direttiva (UE) 2019/713 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti". D. Lgs. 8 novembre 2021, n. 184.	9.12

9.2 – Analisi iniziale

La matrice seguente identifica le aree aziendali (funzioni e processi) oggetto di indagine in riferimento ai rischi specifici.

Funzioni/Aree	Processi, fasi e attività	Casistica
Amministrazione	Processi di pagamento con carte di credito e consuntivazione spese	1

Processo **Amministrativo**				Giudizio Preliminare [2]	Controlli Esistenti						Valutazione Controlli [3]	Ruolo della Funzione					
Sigla Area/Funz.	N. Fase/Attività	Cod. Reato	Fattore [1]		Esistenza di Procedure	Aggiornamento Procedure	Esistenza di Deleghe	Conoscenza e Comunicazione	Suddivisione Compiti	Controlli e Monitoraggi		Operativo	Decisionale	Autorizzativo	Monitoraggio	Sanzionatorio	*Training*
AMM	1	9	I, E, D	B	☒	☒	☑	☒	☑	☑	E	☑	☒	☒	☑	☒	☒

1 I = Interno, E = Esterno, D = Decisionale. **2** Giudizio preliminare rischio reato: A = Alto, M = Medio, B = Basso, I = Inesistente. **3** Valutazione efficacia e adeguatezza dei controlli: I = Inefficaci, M = da migliorare, E = Efficaci, N = Non Esistenti. 4 ☒ = Elemento non presente; ☑ = Elemento Presente.

Annotazioni.

La nuova fattispecie introdotta dal D. Lgs. 8 novembre 2021, n. 184 non è più rivolta solo alla punizione delle condotte aventi ad oggetto "carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o servizi", ma, più in generale, di quelle riguardanti anche "ogni altro mezzo di pagamento diverso dal contante". Per la definizione di tale concetto, poi, viene in soccorso l'art. 1 del D. Lgs. n. 184/2021; la norma amplia il concetto includendovi "ogni dispositivo, oggetto o *record* protetto, materiale o immateriale, o una loro combinazione, diverso dalla moneta a corso legale, che, da solo o unitamente a una procedura o a una serie di procedure, permette al titolare o all'utente di trasferire denaro o valore monetario, anche attraverso mezzi di scambio digitali".

L'ampliamento dell'oggetto sembra dunque muoversi in due direzioni: da un lato, il fatto di ricomprendere i mezzi di pagamento immateriali consente di sanzionare anche le condotte aventi ad oggetto account di mezzi di pagamento digitali aventi una diffusione sempre più ampia, come Satispay o Paypal, a prescindere dall'esistenza di un documento fisico; dall'altro, lo stesso art. 1 del D. Lgs. n. 184/2021, nel definire i "mezzi di scambio digitali", ricomprende anche la "valuta digitale", a sua volta individuata come "una rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è legata necessariamente a una valuta legalmente istituita e non possiede lo status giuridico di valuta o denaro, ma è accettata da persone fisiche o giuridiche come mezzo di scambio,

e che può essere trasferita, memorizzata e scambiata elettronicamente". Attraverso questa serie di richiami, di fatto, sembrerebbe che le fattispecie di cui all'art. 493-ter c.p. vengano estese a colpire non solo le condotte aventi ad oggetto mezzi di pagamento digitali attraverso cui viene scambiata moneta elettronica avente corso legale, ma anche le c.d. cripto valute, prive di valore legale ma socialmente sempre più accettate come mezzi di pagamento.

Lo stesso art. 2 del D. Lgs. n. 184/2021 introduce anche una nuova fattispecie all'interno del c.p., all'art. 493-quater, rubricato "Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti". Come emerge già dalla rubrica, si tratta di un reato prodromico alla commissione di ulteriori reati concernenti mezzi di pagamento diversi dai contanti; la norma – che rappresenta l'attuazione dell'art. 7 della già citata Dir. 2019/713/UE – incrimina infatti la produzione e varie altre condotte di trasferimento di "apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere reati riguardanti gli strumenti di pagamento diversi dai contanti o sono specificamente adattati al medesimo scopo". Oltre che dall'oggetto materiale del reato, la destinazione allo scopo di commettere reati relativi ai mezzi di pagamento diversi dal contante emerge anche dal dolo specifico, che si sostanzia nel fine di fare uso di tali strumenti, o di consentire ad altri di farne uso, per la commissione di tali reati.

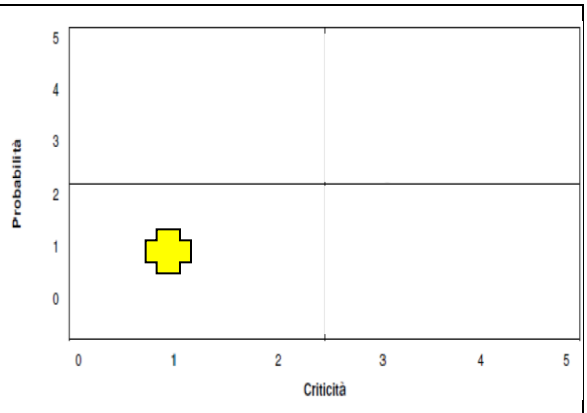
9.3 – Valutazione del Rischio

Si considerino praticamente nulli rischi di reati di Falsità in monete, carte di credito, valori di bollo in quanto i servizi erogati da Etjca S.p.A. non contemplano attività che possano ricondurre a fenomeni ad alta incidenza di tali fattispecie di reati. Esiste un residuale rischio riconducibile all'utilizzo di carte di credito prepagate da parte delle Filiali e di consuntivazione delle spese di trasferte. Tuttavia, i controlli esistenti sono adeguati e commisurati al rischio in quanto il Responsabile dell'Amministrazione ha l'opportunità di verificare in tempo reale le transazioni tramite *home banking.* Le richieste di accredito sulla carta e le spese di trasferta sono in ogni caso motivate dall'utilizzatore. Infine, non si segnalano prassi legati all'utilizzo di forme di trasferimento di denaro con utilizzo di apparecchiature, dispositivi o programmi informatici.

Nell'ambito dei singoli rischi di reato, potenzialmente attivi ognuna delle aree aziendali analizzate, se ne valuta la *magnitudo* di ognuno di essi sulla base delle variabili: probabilità e impatto e, sulla base del valore ottenuto e degli scostamenti, si definisce un piano operativo definendo innanzitutto le tipologie di misure preventive e di controllo da attuare.

Casistica 1. Si consideri l'Area AMM nell'ambito dei processi di pagamento con carte di credito e consuntivazione spese.

Probabilità							
Molto alta	0,45	0,00	2,25	4,50	9,00	18,00	36,00
Alta	0,35	0,00	1,75	3,50	7,00	14,00	28,00
Media	0,25	0,00	1,25	2,50	5,00	10,00	20,00
Bassa	0,15	0,00	0,75	1,50	3,00	6,00	12,00
Molto bassa	0,05	0,00	0,25	0,50	1,00	2,00	4,00
Nulla	0,00	0,00	0,00	0,00	0,00	0,00	0,00
		0	5	10	20	40	80
		Nullo	Molto basso	Basso	Medio	Alto	Molto alto
		Impatto					



Probabilità	Impatto	Indice di Valutazione:
0,05	**5**	**0,25**

La Magnitudo si ottiene moltiplicando le variabili P e I (**M = P * I**); da cui ne deriva che l'Esposizione che può essere classificata **Bassa**, **Media** o **Elevata**. Strategie di *risk response*. Per un rischio alto: **evitare** il rischio (*risk avoidance*), per un rischio medio: **limitare** il rischio (*risk reduction*) o **trasferire** il rischio (*risk transferring/sharing*), per il rischio basso: **accettare** il rischio (*risk acceptance*).

Annotazioni sulla valutazione. In considerazione della limitata criticità si considerano più che adeguati gli attuali controlli esercitati dall'Amministrazione.

9.4 – Misure e Procedure

Sulla base dei rischi rilevati si decide di non approvare specifiche azioni preventive ma di attivare controlli consuntivi sul rischio residuale.

Casistica	Responsabile	Descrizione attività di controllo, risorse, strumenti
1	Direzione/AMM	Trasmissione del *report* di certificazione del bilancio e relativi esiti
1	O.d.V.	Consegnare/esporre/pubblicare il Codice Etico.
1	O.d.V.	Formazione/informazione specifica per il personale
1	O.d.V.	Organizzazione di canali d'informazione tra O.d.V. e parti interessate su casi ritenuti a rischio in applicazione della Procedura PRT 03 - Protocollo segnalazioni di illeciti e irregolarità
1	O.d.V.	L'O.d.V. deve acquisire informazioni in merito all'efficacia delle azioni adottate, eventualmente prescrivere azioni integrative e informare il vertice aziendale.
1	O.d.V.	Redazione di Piano Annuale e consuntivo su Relazione Finale (§ 7 Parte Generale)

CAPITOLO 10: Reati di Ricettazione, Riciclaggio e Autoriciclaggio

10.1 – Principali riferimenti normativi

Articoli di Legge	Cod.
Art. 648 c.p. – reato di ricettazione	10.1
Art. 648 bis c.p. – reato di riciclaggio	10.2
Art. 648 ter c.p. – Impiego di denaro, beni o utilità di illecita provenienza	10.3
Legge n. 186 Articolo 3 del 15/12/2014 con modifica del Art. 648 ter.1 c.p. in materia di autoriciclaggio	10.4
Legge 27 maggio 2015, n. 69 - Disposizioni in materia di delitti contro la pubblica amministrazione, di associazioni di tipo mafioso e di falso in bilancio.	10.5
D.Lgs. 8 novembre 2021, n. 195 relativo all'attuazione della Direttiva 2018/1673 sulla lotta al riciclaggio mediante diritto penale.	10.6

Si applica la pena della reclusione da due a otto anni e della multa da euro 5.000 a euro 25.000 a 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.

Si applica la pena della reclusione da uno a quattro anni e della multa da euro 2.500 a euro 12.500 se il denaro, i beni o le altre utilità provengono dalla commissione di un delitto non colposo punito con la reclusione inferiore nel massimo a cinque anni. Si applicano comunque le pene previste dal primo comma se il denaro, i beni o le altre utilità provengono da un delitto commesso con le condizioni o le finalità di cui all'articolo 7 del decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203, e successive modificazioni.

Fuori dei casi di cui ai commi precedenti, non sono punibili le condotte per cui il denaro, i beni o le altre utilità vengono destinate alla mera utilizzazione o al godimento personale. La pena è aumentata quando i fatti siano commessi nell'esercizio di un'attività bancaria o finanziaria o di altra attività professionale. La pena è diminuita fino alla metà per chi si sia efficacemente adoperato per evitare che le condotte siano portate a conseguenze ulteriori o per assicurare le prove del reato e l'individuazione dei beni, del denaro e delle altre utilità provenienti dal delitto. Si applica l'ultimo comma dell'articolo 648».

Più recentemente, il D.Lgs. n. 195/2021, attuativo della Direttiva 2018/1673 sul riciclaggio, armonizzando la normativa degli stati dell'Unione Europea ha ampliato la casistica di reati presupposto dei delitti di ricettazione, riciclaggio, autoriciclaggio e impiego di denaro, beni o utilità di provenienza illecita (art. 25-octies D.Lgs. 231/2001) comprendendo anche fatti riguardanti denaro o cose provenienti da contravvenzione e, nel caso di riciclaggio e autoriciclaggio, anche i delitti colposi.

10.2 – Analisi iniziale

Reato di riciclaggio. La responsabilità amministrativa dell'ente per i reati previsti dagli art. 648, 648-bis e 648-ter, c.p. è limitata alle ipotesi in cui il reato sia commesso nell'interesse o a vantaggio dell'ente medesimo. Considerato che le fattispecie delittuose in questione possono essere realizzate da chiunque, trattandosi di reati comuni, si dovrebbe ritenere che la ricorrenza del requisito oggettivo dell'interesse o vantaggio vada esclusa ogni qual volta non vi sia attinenza tra la condotta incriminata e l'attività d'impresa esercitata dall'ente.

Tale attinenza, ad esempio, potrebbe ravvisarsi nell'ipotesi di acquisto di beni produttivi provenienti da un delitto di furto, ovvero nel caso di utilizzazione di capitali illeciti per l'aggiudicazione di un appalto, ecc. Viceversa, non è ravvisabile l'interesse o il vantaggio per l'ente nell'ipotesi in cui l'apicale o il dipendente acquistino beni che non abbiano alcun legame con l'esercizio dell'impresa in cui operano. Lo stesso può dirsi per l'impiego di capitali in attività economiche o finanziarie che esorbitano rispetto all'oggetto sociale.

Peraltro, anche nel caso in cui l'oggetto materiale della condotta di ricettazione o di riciclaggio, ovvero l'attività economica o finanziaria nel caso del reato ex art. 648-ter c.p., siano pertinenti rispetto alla specifica attività d'impresa, occorre pur sempre un accertamento in concreto da parte del giudice, da condurre caso per caso, circa la sussistenza dell'interesse o del vantaggio per l'ente.

Reato di autoriciclaggio. Il nuovo reato di autoriciclaggio sanziona il comportamento di chi abbia commesso o concorso a commettere un delitto non colposo, successivamente alla sostituzione, trasferimento, impiego in attività economiche, finanziarie, speculative o imprenditoriali, denaro, beni o altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare l'identificazione della loro provenienza delittuosa.

Questa fattispecie delittuosa si ricollega nella pratica ai reati ascrivibili alle false comunicazioni sociali (ved. § 2). Infatti non è inverosimile che dal reato societario possa derivare un risparmio di denaro (a vantaggio e nell'interesse dell'Agenzia) il quale poi venga successivamente reimpiegato o trasferito. Ciò potrebbe avvenire sia perché, per esempio, non sono stati dichiarati ricavi (che possono superare la soglia prevista per il delitto fiscale, ma avendone omessa l'iscrizione a bilancio è configurato il delitto di falso in bilancio), sia in concorso ulteriore anche con il reato tributario allorché si superi la soglia di punibilità. Il rischio è quindi che con un'unica condotta possa commettersi contemporaneamente i reati di falso in bilancio, quello tributario e quello di autoriciclaggio (anche se, tuttavia, le pene irrogabili ai soggetti economici non quotati in borsa sono meno severe). Tuttavia, allo stato attuale, la giurisprudenza non è ancora ben definita in quanto, poiché l'atto di falso in bilancio e frode fiscale sono reati presupposto rispetto al successivo reato di occultamento per cui potrebbe emergere il principio di *nemo bis in idem* (per cui nessuno può essere giudicato e condannato due volte per uno stesso comportamento delittuoso).

La seguente matrice identifica le aree (funzioni e processi) oggetto di indagine in riferimento ai rischi specifici.

Funzioni/Aree	Processi, fasi e attività	Casistica
Consiglio di Amministrazione	Processo di esposizione di documenti contabili, bilanci e comunicazioni a Soci e Sindaci	1
Amministrazione	Gestione dei rapporti e dei flussi finanziari in entrata (gestione degli incassi) e in uscita intrattenuti con soggetti terzi. Gestione vendite beni e alienazione cespiti	1
Approvvigionamenti	Gestione degli approvvigionamenti di beni e servizi	1

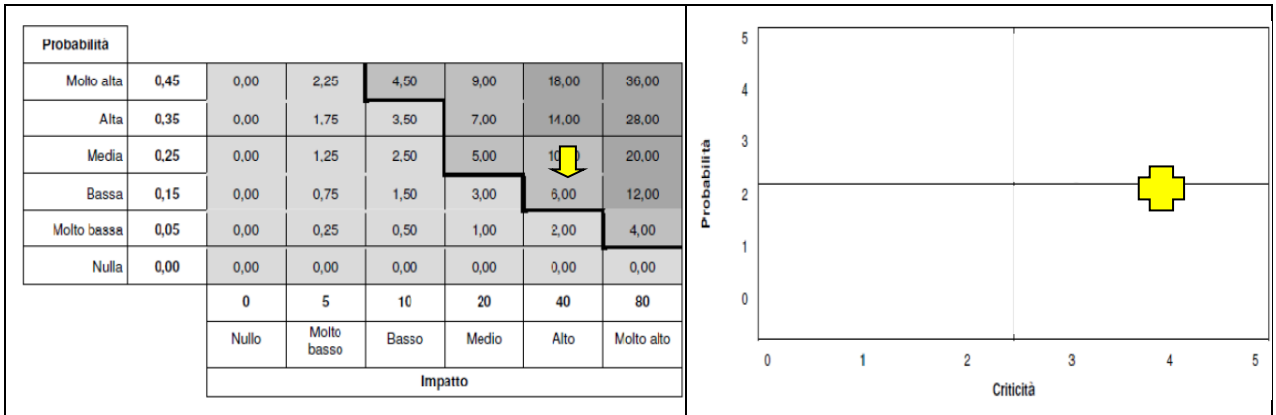
Processo **Processi finanziari**					Controlli Esistenti							Ruolo della Funzione					
Sigla Area/Funz.	N. Fase/Attività	Cod. Reato	Fattore [1]	Giudizio Preliminare [2]	Esistenza di Procedure	Aggiornamento Procedure	Esistenza di Deleghe	Conoscenza e Comunicazione	Suddivisione Compiti	Controlli e Monitoraggi	Valutazione Controlli [3]	Operativo	Decisionale	Autorizzativo	Monitoraggio	Sanzionatorio	*Training*
C.d.A.	1	10	I, E, D	M	☒	☒	☑	☑	☑	☑	M	☑	☑	☑	☑	☑	☒
AMM	2	10	I, E, D	B	☒	☒	☑	☑	☑	☑	E	☑	☑	☑	☑	☒	☒
ACQ	5	10	I, E, D	B	☑	☑	☑	☑	☑	☑	E	☑	☑	☒	☑	☒	☒

1 I = Interno, E = Esterno, D = Decisionale. **2** Giudizio preliminare rischio reato: A = Alto, M = Medio, B = Basso, I = Inesistente. **3** Valutazione efficacia e adeguatezza dei controlli: I = Inefficaci, M = da migliorare, E = Efficaci, N = Non Esistenti. 4 ☒ = Elemento non presente; ☑ = Elemento Presente.

10.3 – Valutazione del Rischio

Nell'ambito dei singoli rischi di reato, potenzialmente attivi in ognuna delle aree aziendali analizzate, se ne valuta la *magnitudo* di ognuno di essi sulla base delle variabili: probabilità e impatto e, sulla base del valore ottenuto e degli scostamenti, si definisce un piano operativo definendo innanzitutto le tipologie di misure preventive e di controllo da attuare.

Casistica 1. Si considerino tutte le aree sopra indicate nell'ambito unico dei processi economici e finanziari d'impresa.



Probabilità	Impatto	Indice di Valutazione:
0,15	**40**	**6**

La Magnitudo si ottiene moltiplicando le variabili P e I (**M = P * I**); da cui ne deriva che l'Esposizione che può essere classificata **Bassa**, **Media** o **Elevata**.

Strategie di *risk response*. Per un rischio alto: **evitare** il rischio (*risk avoidance*), per un rischio medio: **limitare** il rischio (*risk reduction*) o **trasferire** il rischio (*risk transferring/sharing*), per il rischio basso: **accettare** il rischio (*risk acceptance*).

Annotazioni sulla valutazione

Reati di riciclaggio e di autoriciclaggio. Per quanto attiene al reato di riciclaggio si consideri un'incidenza del rischio bassa e circoscritta in quanto, viste le tipologie di sevizi erogati, difficilmente potrebbe essere commesso un simile reato negli interessi dell'Agenzia. Inoltre, gli incassi avvengono sempre su base bancaria e totalmente tracciabile.

Modalità di commissione reati, rischi e ricadute. Si consideri quanto scritto a riguardo dei reati di falso in bilancio (ved § 2).

Controlli esistenti. Esistono meccanismi di controllo e approvazione del bilancio e della situazione contabile come precedentemente indicato al § 2. In particolare, tutti i flussi finanziari (ciclo attivi e ciclo passivo) sono di fatto totalmente tracciabili a scopi rendicontativi con flussi destinati in conti correnti dedicati (come capita nel caso di progetti finanziati).

10.4 – Misure e Procedure

L'Organismo di Vigilanza effettua periodicamente controlli a campione sulle attività connesse ai «processi sensibili» diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello. A tal fine all'Organismo viene garantito libero accesso a tutta la documentazione aziendale rilevante così come previsto nella Parte Generale del Modello 231. Inoltre, l'Organismo di Vigilanza può attivarsi con specifici controlli a seguito delle segnalazioni ricevute, secondo quanto riportato nella Parte Generale del Modello 231.

In particolare, è compito dell'Organismo di Vigilanza:

a) Verifica della regolarità dei pagamenti, con riferimento alla piena coincidenza tra destinatari/ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni. Tali controlli devono tener conto della sede legale della società controparte (ad es. paradisi fiscali, Paesi a rischio terrorismo, ecc.), degli Istituti di credito utilizzati (sede legale delle banche coinvolte nelle operazioni e Istituti che non hanno insediamenti fisici in alcun Paese) e di eventuali schermi societari e strutture fiduciarie utilizzate per transazioni o operazioni straordinarie.

b) verificare periodicamente il sistema di deleghe in vigore, raccomandando delle modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti al responsabile interno;

c) verificare il rispetto e la corretta applicazione delle prescrizioni previste nei processi sensibili da parte di tutti i soggetti aziendali (es. verifiche sulla Tesoreria sul rispetto delle soglie per i pagamenti per contanti, eventuale utilizzo di libretti al portatore o anonimi per la gestione della liquidità, ecc.);

d) verificare periodicamente, con il supporto delle altre funzioni competenti:

- l'osservanza da parte dei Destinatari delle disposizioni del Decreto;
- la possibilità di effettuare efficaci azioni di controllo nei confronti dei destinatari del Modello al fine di verificare il rispetto delle prescrizioni in esso contenute;
- l'attuazione di meccanismi sanzionatori qualora si accertino violazioni delle prescrizioni: es. previsione di regole disciplinari in materia di prevenzione dei fenomeni di riciclaggio (ved. Codice Etico e Regime Sanzionatorio);

e) indicare al *management* le opportune integrazioni ai sistemi gestionali delle risorse finanziarie, già presenti in ETJCA, con l'introduzione di alcuni accorgimenti suscettibili di rilevare l'esistenza di eventuali flussi finanziari atipici e connotati da maggiori margini di discrezionalità rispetto a quanto ordinariamente previsto.

f) verificare l'applicazione dei controlli preventivi specifici previsti anche in riferimento ai reati nei rapporti con la Pubblica Amministrazione, ai reati societari e ai reati di "*market abuse"*;

g) prevedere l'adozione di adeguati programmi di formazione del personale ritenuto esposto al rischio di riciclaggio.

In ogni caso, oltre ai compiti di controllo conferiti all'O.d.V., prima dell'iter di approvazione del Bilancio, potrebbero essere utili incontri tra C.d.A. e il Responsabile Amministrativo con eventuali approfondimenti e analisi documentali di fattispecie di particolare rilievo e complessità presenti nella bozza predisposta, curando la stesura del relativo verbale.

Sulla base dei rischi rilevati si stabiliscono specifiche azioni preventive, le tempistiche, gli strumenti/risorse e le relative responsabilità.

Casistica	Responsabile	Descrizione attività di controllo, risorse, strumenti
1	O.d.V.	Consegnare/esporre/pubblicare il Codice Etico
1	O.d.V.	Formazione/informazione specifica per il personale
1	Direzione/AMM	Trasmissione del *report* di certificazione del bilancio e relativi esiti
1	O.d.V./*auditor* incaricato	Prevedere che si effettuino controlli (registrati) sui seguenti item: a) astenersi dal realizzare comportamenti che possano in qualsivoglia modo integrare, direttamente o indirettamente, condotte di riciclaggio, autoriciclaggio o di ricettazione e/o possano agevolarne o favorirne la relativa commissione. A tale proposito, integrano le condotte di riciclaggio o di impiego di denaro, beni o altra utilità di provenienza illecita, la sostituzione o il trasferimento del denaro, dei beni o di altra utilità di provenienza illecita, ovvero il compimento di operazioni atte a ostacolare l'identificazione della loro provenienza illecita, mentre integra la condotta della ricettazione l'acquisto o il ricevimento ovvero l'occultamento di denaro o cose provenienti da un qualsiasi reato; b) attraverso le informazioni disponibili, verificare sotto il profilo della onorabilità e affidabilità le controparti commerciali e, più in generale, i clienti con cui si avviassero rapporti d'affari in particolare se localizzati in aree geografiche particolarmente interessate da fenomeni di criminalità organizzata anche di tipo mafioso (tale comportamento è richiesto anche ai fini di prevenire eventuali rapporti con organizzazioni criminali); c) utilizzare nelle transazioni il sistema bancario, richiedendo anche ai clienti che i pagamenti avvengano esclusivamente tramite tale sistema, che consente la tracciabilità dei trasferimenti finanziari; d) vietare l'utilizzo del contante ed effettuare controlli sulle transazioni. è fatto divieto di emettere assegni bancari e postali per importi pari o superiori a 5.000 euro che non rechino l'indicazione del nome o della ragione sociale del beneficiario e la clausola di non trasferibilità. e) eventuale richiesta del DURC a Clienti e Fornitori.
1	O.d.V.	L'O.d.V. deve acquisire informazioni in merito all'efficacia delle azioni adottate, eventualmente prescrivere azioni integrative e informare il vertice aziendale. Al riguardo gestire uno specifico programma di *audit* periodici allo scopo di verificare l'adeguatezza del sistema di interno di controllo dei flussi economici e finanziari
1	O.d.V.	Organizzazione di canali d'informazione tra O.d.V. e parti interessate su casi ritenuti a rischio in applicazione della Procedura PRT 03 - Protocollo segnalazioni di illeciti e irregolarità
1	O.d.V.	Redazione di Piano Annuale e consuntivo su Relazione Finale (§ 7 Parte Generale)

CAPITOLO 11: Reati Ambientali

11.1 – Principali riferimenti normativi

Articoli di Legge	Cod.
Art. 727- bis C.p. - Delitto di danneggiamento di *habitat* all'interno di un sito protetto ;	11.1
Art. 733 – bis C.p. - uccisione o possesso di specie vegetali o animali protette	11.2
Reati previsti dal Decreto Legislativo 3 aprile 2006, n. 152 (artt. 137, 256, 257, 258, 259, 260, 260 bis, 279)	11.3
Reati previsti dalla legge 7 febbraio 1992, n. 150 (artt. 1, 2 , 3 bis e 6)	11.4
Reati previsti dall'articolo 3, comma 6, della legge 28 dicembre 1993, n. 549	11.5
Reati previsti dal Decreto Legislativo 6 novembre 2007, n. 202 (artt. 8 e 9)	11.6

11.2 – Analisi iniziale

La matrice seguente identifica le aree aziendali (funzioni e processi) oggetto di indagine in riferimento ai rischi specifici.

Funzioni/Aree	Processi, fasi e attività	Casistica
Nessuna	Nessun processo	/

Processo /				Giudizio Preliminare [2]	Controlli Esistenti						Valutazione Controlli [3]	Ruolo della Funzione					
Sigla Area/Funz.	N. Fase/Attività	Cod. Reato	Fattore [1]		Esistenza di Procedure	Aggiornamento Procedure	Esistenza di Deleghe	Conoscenza e Comunicazione	Suddivisione Compiti	Controlli e Monitoraggi		Operativo	Decisionale	Autorizzativo	Monitoraggio	Sanzionatorio	*Training*
/	/	11	I	I	☒	☒	☒	☒	☒	☒	N	☒	☒	☒	☒	☒	☒

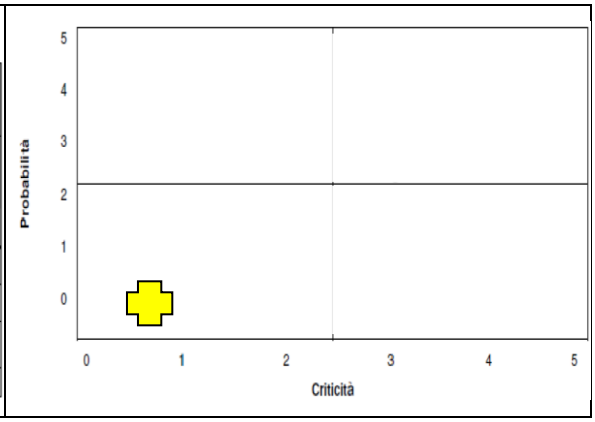
1 I = Interno, E = Esterno, D = Decisionale. **2** Giudizio preliminare rischio reato: A = Alto, M = Medio, B = Basso, I = Inesistente. **3** Valutazione efficacia e adeguatezza dei controlli: I = Inefficaci, M = da migliorare, E = Efficaci, N = Non Esistenti. 4 ☒ = Elemento non presente; ☑ = Elemento Presente.

Annotazioni. Se si eccettua lo smaltimento dei *toner* (per il quale si seguono le normative comunali applicabili), si considerino praticamente nulli i rischi di reati di natura ambientale in quanto i servizi erogati da Etjca S.p.A. non contemplano attività che possano ricondurre a tali fattispecie di reati. Non esistono estremi per rilevare rischi residui e di conseguenza non esistono procedure e controlli specifici.

11.3 – Valutazione del Rischio

Nell'ambito dei singoli rischi di reato, potenzialmente attivi ognuna delle aree aziendali analizzate, se ne valuta la *magnitudo* di ognuno di essi sulla base delle variabili: probabilità e impatto e, sulla base del valore ottenuto e degli scostamenti, si definisce un piano operativo definendo innanzitutto le tipologie di misure preventive e di controllo da attuare.

Probabilità							
Molto alta	0,45	0,00	2,25	4,50	9,00	18,00	36,00
Alta	0,35	0,00	1,75	3,50	7,00	14,00	28,00
Media	0,25	0,00	1,25	2,50	5,00	10,00	20,00
Bassa	0,15	0,00	0,75	1,50	3,00	6,00	12,00
Molto bassa	0,05	0,00	0,25	0,50	1,00	2,00	4,00
Nulla	0,00	0,00	0,00	0,00	0,00	0,00	0,00
		0	5	10	20	40	80
		Nullo	Molto basso	Basso	Medio	Alto	Molto alto
		Impatto					



Probabilità	Impatto	Indice di Valutazione:
0	**0**	**0**

La Magnitudo si ottiene moltiplicando le variabili P e I (**M = P * I**); da cui ne deriva che l'Esposizione che può essere classificata **Bassa**, **Media** o **Elevata**. Strategie di *risk response*. Per un rischio alto: **evitare** il rischio (*risk avoidance*), per un rischio medio: **limitare** il rischio (*risk reduction*) o **trasferire** il rischio (*risk transferring/sharing*), per il rischio basso: **accettare** il rischio (*risk acceptance*).

Annotazioni sulla valutazione. Non esistono processi a rischio e, di conseguenza, non si attivano controlli specifici.

11.4 – Misure e Procedure

Sulla base dei rischi rilevati si decide di non approvare specifiche azioni preventive.

Casistica	Responsabile	Descrizione attività di controllo, risorse, strumenti
/	/	/

CAPITOLO 12: Criminalità organizzata, terrorismo, eversione, reati transnazionali

12.1 – Principali riferimenti normativi

Articoli di Legge	Cod.
art. 416 c. 6 c.p., associazione per delinquere finalizzata alla riduzione o mantenimento in schiavitù, alla tratta di persone, all'acquisto e all'alienazione di schiavi, alla commissione di reati concernenti l'immigrazione clandestina;	12.1
art. 416 bis c.p., associazione per delinquere di stampo mafioso;	12.2
art. 416 ter c.p., scambio elettorale politico-mafioso;	12.3
art. 630 c.p., sequestro di persona a scopo di estorsione;	12.4
art. 74 D.P.R. 309/1990, associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope	12.5
Legge 16 marzo 2006, n. 146, art. 10	12.6
art. 630 c.p. reato di sequestro di persona a scopo di rapina o di estorsione	12.7
DPR 43/73, art. 291 quater	12.8
art. 377 bis c.p., Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria.	12.9
art. 378 c.p., Favoreggiamento personale	12.10

12.2 – Analisi iniziale

La matrice seguente identifica le aree aziendali (funzioni e processi) oggetto di indagine in riferimento ai rischi specifici.

Funzioni/Aree	Processi, fasi e attività	Casistica
Nessuna	Nessun processo	/

Processo /				Giudizio Preliminare [2]	Controlli Esistenti						Valutazione Controlli [3]	Ruolo della Funzione					
Sigla Area/Funz.	N. Fase/Attività	Cod. Reato	Fattore [1]		Esistenza di Procedure	Aggiornamento Procedure	Esistenza di Deleghe	Conoscenza e Comunicazione	Suddivisione Compiti	Controlli e Monitoraggi		Operativo	Decisionale	Autorizzativo	Monitoraggio	Sanzionatorio	*Training*
/	/	12	I	I	☒	☒	☒	☒	☒	☒	N	☒	☒	☒	☒	☒	☒

1 I = Interno, E = Esterno, D = Decisionale. **2** Giudizio preliminare rischio reato: A = Alto, M = Medio, B = Basso, I = Inesistente. **3** Valutazione efficacia e adeguatezza dei controlli: I = Inefficaci, M = da migliorare, E = Efficaci, N = Non Esistenti. 4 ☒ = Elemento non presente; ☑ = Elemento Presente.

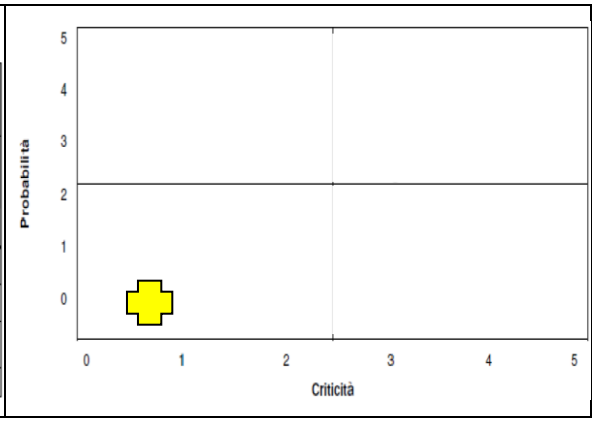
Annotazioni. Si considerino praticamente nulli i rischi di reati di natura ambientale in quanto i servizi erogati da Etjca S.p.A. non contemplano attività che possano ricondurre a tali fattispecie di reati.

Non esistono estremi per rilevare rischi residui e di conseguenza non esistono procedure e controlli specifici.

12.3 – Valutazione del Rischio

Nell'ambito dei singoli rischi di reato, potenzialmente attivi ognuna delle aree aziendali analizzate, se ne valuta la *magnitudo* di ognuno di essi sulla base delle variabili: probabilità e impatto e, sulla base del valore ottenuto e degli scostamenti, si definisce un piano operativo definendo innanzitutto le tipologie di misure preventive e di controllo da attuare.

Probabilità							
Molto alta	0,45	0,00	2,25	4,50	9,00	18,00	36,00
Alta	0,35	0,00	1,75	3,50	7,00	14,00	28,00
Media	0,25	0,00	1,25	2,50	5,00	10,00	20,00
Bassa	0,15	0,00	0,75	1,50	3,00	6,00	12,00
Molto bassa	0,05	0,00	0,25	0,50	1,00	2,00	4,00
Nulla	0,00	0,00	0,00	0,00	0,00	0,00	0,00
		0	5	10	20	40	80
		Nullo	Molto basso	Basso	Medio	Alto	Molto alto
		Impatto					



Probabilità	Impatto	Indice di Valutazione:
0	**0**	**0**

La Magnitudo si ottiene moltiplicando le variabili P e I (**M = P * I**); da cui ne deriva che l'Esposizione che può essere classificata **Bassa**, **Media** o **Elevata**. Strategie di *risk response*. Per un rischio alto: **evitare** il rischio (*risk avoidance*), per un rischio medio: **limitare** il rischio (*risk reduction*) o **trasferire** il rischio (*risk transferring/sharing*), per il rischio basso: **accettare** il rischio (*risk acceptance*).

Annotazioni sulla valutazione. Non esistono processi a rischio e, di conseguenza, non si attivano controlli specifici.

12.4 – Misure e Procedure

Sulla base dei rischi rilevati si decide di non approvare specifiche azioni preventive.

Casistica	Responsabile	Descrizione attività di controllo, risorse, strumenti
/	/	/

CAPITOLO 13: Reato di corruzione tra privati

13.1 – Principali riferimenti normativi

Articoli di Legge	Cod.
art. 2635 c.c.	13.1
art. 2635-bis	13.2
Decreto Legislativo 15 marzo 2017, n. 3	

13.2 – Analisi iniziale

Il Decreto Legislativo 15 marzo 2017, n. 3 individua i soggetti punibili ricomprendono ora tutti quanti svolgono funzioni direttive ed anche coloro che pongono in essere la condotta per interposta persona. La condotta punita è stata estesa, oltre che alla sollecitazione e ricezione, anche all'accettazione della promessa di ricevere denaro o altra utilità non dovuti. La finalità del reato è quella di compiere oppure omettere un atto in violazione degli obblighi dell'ufficio o di fedeltà e non è più richiesta la prova di un danno per la società. È rimasta invece la procedibilità a querela di parte, salvo che dal fatto derivi una distorsione della concorrenza.

Corruzione tra privati. La condotta illecita consiste nel sollecitare o ricevere, anche per interposta persona, per sé o per altri, denaro o altra utilità non dovuti, o accettarne la promessa, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà. La fattispecie sembra dunque costruita in termini di reato di mera condotta, senza cioè la previsione di un evento di danno.

Istigazione alla corruzione tra privati. L'art. 2635-ter prevede, in caso di condanna per il reato di corruzione tra privati, l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese nei confronti di chi abbia già riportato una precedente condanna per il medesimo reato o per l'istigazione di cui al comma 2 dell'art. 2635-bis. Sono previsti inasprimenti delle sanzioni per l'ente nel caso in cui il corruttore sia soggetto che abbia agito in nome e nell'interesse dell'ente, prevedendo l'applicazione delle sanzioni interdittive. Rimane punito solo l'ente (che può essere anche una associazione) che abbia commesso corruzione attiva. L'istigazione alla corruzione tra privati è una speciale ipotesi di tentativo, inserita con il d.lgs. 38/2017, in attuazione di una decisione quadro del Consiglio dell'Unione Europea: tale fattispecie risulta integrata in seguito alla mancata accettazione dell'offerta o della promessa.

Ai sensi dell'art. 2635 bis c.p. è punito con la pena stabilita nel primo comma dell'art. 2635 c.p. ridotta di un terzo, quando l'offerta o la promessa non sia accettata, chiunque offre o promette denaro o altre utilità non dovuti agli amministratori, direttori generali, dirigenti preposti alla redazione di documenti contabili societari, sindaci e liquidatori, di società o enti privati, nonché a chi svolge in essi attività lavorativa che comporti l'esercizio di funzioni direttive, affinché compia od ometta un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà.

La stessa pena si applica, qualora la sollecitazione non sia accettata, agli stessi soggetti di cui al comma 1 che sollecitano per sé o per altri ed anche per interposta persona una promessa o dazione di denaro o di altra utilità per compiere od omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà.

La seguente matrice identifica le aree aziendali oggetto di indagine in riferimento ai rischi specifici.

Funzioni/Aree	Processi, fasi e attività	N. casistica
C.d.A./ Collegio Sindaci	Processo di formazione del bilancio e relativi controlli e di gestione delle comunicazioni sociali	1, 2, 3
AMM	Ciclo attivo e passivo. Rapporti con banche/finanziarie/creditori.	1, 2, 3
AMM	Selezione e assunzione di personale	1, 2, 3

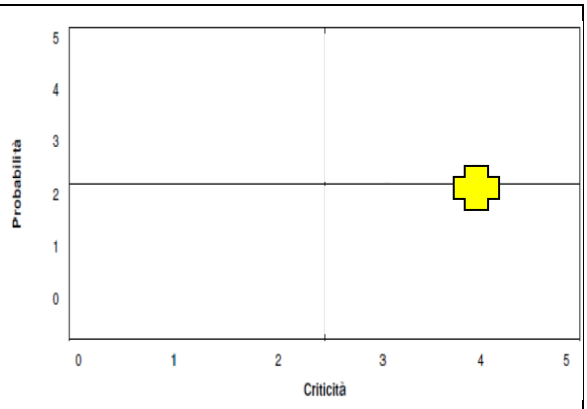
Processo **Processi C.d.A.**				Giudizio Preliminare [2]	Controlli Esistenti						Valutazione Controlli [3]	Ruolo della Funzione					
Sigla Area/Funz.	N. Fase/Attività	Cod. Reato	Fattore [1]		Esistenza di Procedure	Aggiornamento Procedure	Esistenza di Deleghe	Conoscenza e Comunicazione	Suddivisione Compiti	Controlli e Monitoraggi		Operativo	Decisionale	Autorizzativo	Monitoraggio	Sanzionatorio	*Training*
C.d.A.	1	13	I, D	M	☑	☑	☑	☑	☑	☑	M	☑	☑	☑	☒	☑	☒
SND	1	13	I, D	M	☑	☑	☑	☑	☑	☑	M	☑	☒	☒	☑	☒	☒
AMM	1	13	I, D	M	☑	☑	☑	☑	☑	☑	M	☑	☒	☒	☑	☒	☒

1 I = Interno, E = Esterno, D = Decisionale. **2** Giudizio preliminare rischio reato: A = Alto, M = Medio, B = Basso, I = Inesistente. **3** Valutazione efficacia e adeguatezza dei controlli: I = Inefficaci, M = da migliorare, E = Efficaci, N = Non Esistenti. 4 ☒ = Elemento non presente; ☑ = Elemento Presente.

13.3 – Valutazione del Rischio

Nell'ambito dei singoli rischi di reato, potenzialmente attivi in ognuna delle aree aziendali analizzate, se ne valuta la *magnitudo* di ognuno di essi sulla base delle variabili: probabilità e impatto e, sulla base del valore ottenuto e degli scostamenti, si definisce un piano operativo definendo innanzitutto le tipologie di misure preventive e di controllo da attuare.

Probabilità							
Molto alta	0,45	0,00	2,25	4,50	9,00	18,00	36,00
Alta	0,35	0,00	1,75	3,50	7,00	14,00	28,00
Media	0,25	0,00	1,25	2,50	5,00	10,00	20,00
Bassa	0,15	0,00	0,75	1,50	3,00	6,00	12,00
Molto bassa	0,05	0,00	0,25	0,50	1,00	2,00	4,00
Nulla	0,00	0,00	0,00	0,00	0,00	0,00	0,00
		0	5	10	20	40	80
		Nullo	Molto basso	Basso	Medio	Alto	Molto alto
		Impatto					



Probabilità	Impatto	Indice di Valutazione:
0,15	**40**	**6**

La Magnitudo si ottiene moltiplicando le variabili P e I (**M = P * I**); da cui ne deriva che l'Esposizione che può essere classificata **Bassa**, **Media** o **Elevata**. Strategie di *risk response*. Per un rischio alto: **evitare** il rischio (*risk avoidance*), per un rischio medio: **limitare** il rischio (*risk reduction*) o **trasferire** il rischio (*risk transferring/sharing*), per il rischio basso: **accettare** il rischio (*risk acceptance*).

Modalità e contesti di commissione del reato (Casistiche 1, 2, 3)

Il reato di corruzione tra privati potrebbe essere commesso da parte di un membro del C.d.A. e/o di Responsabili della Funzione interessata (figure apicali), nonché da sottoposti alla direzione e alla vigilanza di tali soggetti (sottoposti).

Esempi di rischi di commessione reato si possono configurare:

- nella vendita di beni ad altra società, con lo scopo di ottenere dal cliente la conclusione di un contratto;
- nell'esecuzione di prestazioni di servizi ad altra società, al fine di corrompere un concorrente durante la partecipazione a una gara privata affinché lo stesso presenti condizioni peggiori.
- nei confronti dei fornitori della Società per ottenere beni/servizi a migliori condizioni e/o a prezzi più favorevoli.
- mediante l'assunzione da parte della Società di persone a conoscenza di segreti industriali di Società concorrenti al fine di ottenere la rivelazione di tali segreti.
- nei rapporti con i creditori con lo scopo di concludere transazioni più vantaggiose per la Società ovvero al fine di ritardare l'azione esecutiva.
- potrebbe essere commesso, da un lato, nei rapporti con le banche, mediante la corruzione di funzionari per ottenere benefici economici, dall'altro, nei rapporti con le finanziarie, tramite la corruzione di un dipendente al fine di evitare che la Società sia segnalata.
- potrebbe perpetrarsi un reato di corruzione nei riguardi dei soggetti preposti al controllo del bilancio (sindaci o società di revisione).

13.4 – Misure e Procedure

Preliminarmente, si evidenzia da un lato che il Modello 231 ha una sezione dedicata ai rapporti illeciti con la P.A. al cui interno hanno un ruolo preminente i reati di corruzione (Ved. Cap. 1), dall'altro ETJCA adotta e persegue politiche aziendali finalizzate alla prevenzione dei reati di corruttela espresse nel Codice Etico vigente.

Inoltre, taluni principi procedurali di comportamento precedentemente indicati in altri capitoli della Parte Speciale e all'interno del Codice Etico sono idonei a minimizzare il rischio di reato oggetto di questo capitolo Inoltre sono previste procedure/protocolli specifici del modello che trattano i medesimi ambiti.

Al fine, poi, di garantire il più possibile la prevenzione del compimento da parte dei Destinatari del Modello di azioni che possono concretizzare la fattispecie contemplata nella Parte Speciale, la Società deve adottare e predisporre una serie di principi generali di comportamento, fermo restando il rispetto del Modello, del Codice Etico e delle procedure.

In particolare, ai destinatari è fatto divieto di:

- ricevere, pretendere, corrispondere e offrire direttamente o indirettamente, compensi di qualunque natura, regali, vantaggi economici o altra utilità da, o a, un soggetto privato e/o l'ente da esso direttamente o indirettamente rappresentato che: i) eccedano un modico valore e i limiti di ragionevoli prassi di cortesia e, comunque, ii) siano suscettibili di essere interpretati come volti a influenzare indebitamente i rapporti tra la Società e il predetto soggetto e/o l'ente da esso direttamente o indirettamente rappresentato, a prescindere dalla finalità di perseguimento, anche esclusivo, dell'interesse o del vantaggio della Società;
- corrispondere pagamenti di modico valore non ufficiali, effettuati allo scopo di velocizzare, favorire o assicurare l'effettuazione di un'attività di *routine* o comunque prevista nell'ambito dei doveri dei soggetti privati con cui la Società si relaziona;
- utilizzare fondi o mezzi personali allo scopo di aggirare l'applicazione dei contenuti della Presente Parte Speciale;
- sottoscrivere contratti superiori al valore soglia indicato nella procura, ove non autorizzati per iscritto dai vertici.

Inoltre, ogni attività svolta nelle aree sensibili sopra indicate, deve essere accuratamente e regolarmente riflessa nei documenti contabili. È, infatti, responsabilità della Società redigere documenti contabili che riflettano con un dettaglio ragionevole ciascuna operazione, nonché stabilire e eseguire controlli adeguati al fine di garantire che:

- le operazioni siano effettive ed eseguite solo a fronte di un'autorizzazione del vertice aziendale;
- le operazioni siano registrate al fine di permettere la redazione del bilancio in conformità con i principi contabili;
- il valore dei beni inseriti a bilancio sia riscontrato, con una certa periodicità, con gli inventari e siano adottate appropriate misure in riferimento alle differenze riscontrate.

Nessuna pratica qualificabile come di natura corruttiva può essere giustificata o tollerata quale "consuetudinaria" nel settore di *business*.

Non è consentito imporre o accettare alcuna prestazione ove la stessa può essere realizzata, solamente, pregiudicando i valori ed i principi del Codice Etico o violando le procedure del Modello applicabili e le normative.

L'attività dell'Organismo di Vigilanza é svolta in stretta collaborazione con i vari responsabili delle Aree interessate. Pertanto, dovranno essere previsti flussi informativi costanti tra tali soggetti e l'O.d.V. al fine di ottimizzare le attività di verifica. I controlli effettuati dall'O.d.V. sono diretti a verificare la conformità delle attività aziendali ai principi espressi nella presente Parte Speciale e, in particolare, alle procedure interne in essere e a quelle che saranno adottate in futuro, in attuazione della presente Parte Speciale.

Casistica	Responsabile	Descrizione attività di controllo, risorse, strumenti
1, 2 e 3	Direzione	Formazione e informazione Funzioni coinvolte e distribuzione del Codice Etico
1, 2 e 3	Direzione	Condivisione Codice Etico e Regime Sanzionatorio.
1, 2 e 3	Direzione	Trasmissione del *report* di certificazione del bilancio e relativi esiti
1, 2 e 3	O.d.V.	Organizzazione di canali d'informazione tra O.d.V. e parti interessate su casi ritenuti a rischio in applicazione della Procedura PRT 03 - Protocollo segnalazioni di illeciti e irregolarità
1, 2 e 3	O.d.V.	Azioni di *Auditing* periodico (almeno un *audit*/anno) e possibilità di verifiche senza preavviso
1, 2 e 3	O.d.V.	Acquisizione di documenti e informazioni in merito all'efficacia delle azioni adottate, eventualmente prescrivere azioni integrative e informare il vertice aziendale.
1, 2 e 3	O.d.V.	Redazione di Piano Annuale e consuntivo su Relazione Finale (§ 7 Parte Generale)

CAPITOLO 14: Reato di favoreggiamento dell'immigrazione clandestina e utilizzo di manodopera irregolare

14.1 – Principali riferimenti normativi

Articoli di Legge	Cod.
Art. 603 bis c.p.	13.1
Direttiva 2009/52/CE	13.2
25 duodecies (Reato Irregolare Immigrazione) Articolo introdotto dal D.Lgs. n. 109/2012 pubblicato sulla G.U. n. 172 del 25 luglio 2012.	13.3
D.Lgs. 25 luglio 1998, n. 286, T.U. testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero.	13.4

14.2 – Analisi iniziale

Il 9 agosto 2012 è entrato in vigore il D.Lgs. 109/2012, il quale amplia i reati presupposto per la responsabilità amministrativa delle persone giuridiche prevista dal d.lgs. 231/2001, in attuazione della direttiva 2009/52/CE, che introduce norme relative a sanzioni e a provvedimenti nei confronti di Datori di Lavoro che impiegano cittadini di Paesi terzi il cui soggiorno è irregolare. È un delitto di natura dolosa, suscettibile di fondare la responsabilità dell'ente nella sola ipotesi aggravata di cui al comma 12 - bis.

La matrice seguente identifica le aree aziendali (funzioni e processi) oggetto di indagine in riferimento ai rischi specifici.

Funzioni/Aree	Processi, fasi e attività	Casistica
Amministrazione	Gestione dei rapporti e dei flussi finanziari in entrata (gestione degli incassi) e in uscita intrattenuti con soggetti terzi.	1
Risorse Umane	Gestione dei rapporti contrattuali con i dipendenti di struttura e somministrati	2
Area Clienti/Filiali	Rapporti contrattuali con i Clienti	3

Processo **Processi finanziari**				Giudizio Preliminare [2]	Controlli Esistenti						Valutazione Controlli [3]	Ruolo della Funzione					
Sigla Area/Funz.	N. Fase/Attività	Cod. Reato	Fattore [1]		Esistenza di Procedure	Aggiornamento Procedure	Esistenza di Deleghe	Conoscenza e Comunicazione	Suddivisione Compiti	Controlli e Monitoraggi		Operativo	Decisionale	Autorizzativo	Monitoraggio	Sanzionatorio	*Training*
AMM	1	14	I, E, D	B	☒	☒	☑	☑	☑	☑	E	☑	☑	☑	☑	☒	☒
RU	2	14	I, E, D	B	☑	☑	☑	☑	☑	☑	E	☑	☑	☒	☑	☒	☒
CLI	3	14	I, E, D	M	☑	☑	☑	☑	☑	☑	M	☑	☑	☒	☑	☒	☒

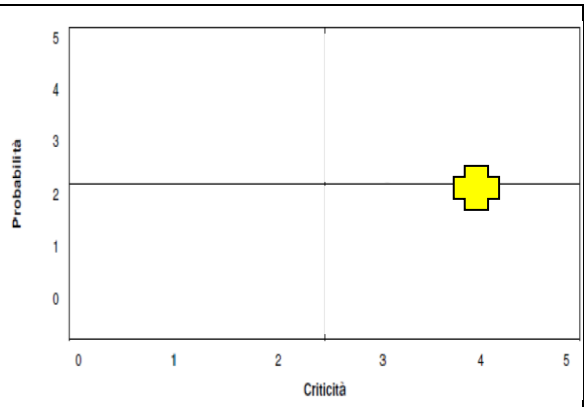
1 I = Interno, E = Esterno, D = Decisionale. **2** Giudizio preliminare rischio reato: A = Alto, M = Medio, B = Basso, I = Inesistente. **3** Valutazione efficacia e adeguatezza dei controlli: I = Inefficaci, M = da migliorare, E = Efficaci, N = Non Esistenti. 4 ☒ = Elemento non presente; ☑ = Elemento Presente.

Annotazioni. L'analisi iniziale indica che l'entità del rischio è da considerarsi molto bassa in quanto non esiste situazione e contratto che possa portare vantaggi e interessi nel compimento di questa fattispecie di reato. Esiste tuttavia un basso rischio a seguito di problematiche legate alla scadenza/sospensione/revoca del permesso di soggiorno per cui si richiede di attivare adeguati controlli presso le Filiali.

14.3 – Valutazione del Rischio

Nell'ambito dei singoli rischi di reato, potenzialmente attivi in ognuna delle aree aziendali analizzate, se ne valuta la *magnitudo* di ognuno di essi sulla base delle variabili: probabilità e impatto e, sulla base del valore ottenuto e degli scostamenti, si definisce un piano operativo definendo innanzitutto le tipologie di misure preventive e di controllo da attuare.

Probabilità							
Molto alta	0,45	0,00	2,25	4,50	9,00	18,00	36,00
Alta	0,35	0,00	1,75	3,50	7,00	14,00	28,00
Media	0,25	0,00	1,25	2,50	5,00	10,00	20,00
Bassa	0,15	0,00	0,75	1,50	3,00	6,00	12,00
Molto bassa	0,05	0,00	0,25	0,50	1,00	2,00	4,00
Nulla	0,00	0,00	0,00	0,00	0,00	0,00	0,00
		0	5	10	20	40	80
		Nullo	Molto basso	Basso	Medio	Alto	Molto alto
		Impatto					



Probabilità	Impatto	Indice di Valutazione:
0,15	**40**	**6**

La Magnitudo si ottiene moltiplicando le variabili P e I (**M = P * I**); da cui ne deriva che l'Esposizione che può essere classificata **Bassa**, **Media** o **Elevata**. Strategie di *risk response*. Per un rischio alto: **evitare** il rischio (*risk avoidance*), per un rischio medio: **limitare** il rischio (*risk reduction*) o **trasferire** il rischio (*risk transferring/sharing*), per il rischio basso: **accettare** il rischio (*risk acceptance*).

Annotazioni sulla valutazione.

Modalità e contesti di commissione del reato

Si considerino i seguenti contesti:

- Stipulazione di contratti di lavoro subordinato (a tempo indeterminato o determinato), parasubordinato e autonomo;
- Situazioni di distacco, contratti di somministrazione, contratti di appalto.

In questi contesti l'unica situazione si riferisce all'utilizzo (anche involontario) di personale non in regola con i permessi di soggiorno.

Rischi e ricadute

Considerando il contesto geografico e il settore in cui opera Etjca, non si configurano particolari rischi nella gestione dei rapporti contrattuali con i dipendenti di struttura e con i lavoratori somministrati. L'entità del rischio è da considerarsi molto bassa in quanto non esistono, nel nostro ambito, situazioni e fattispecie contrattuali che possano portare consistenti vantaggi nel compimento di questa fattispecie di reato, se non a fronte di elevati risch,i in ogni caso non rapportabili ai vantaggi che ne deriverebbero. Questa situazione potrebbe verificarsi soltanto in casi particolari e, tuttavia, nel caso in cui l'attuale sistema di controllo fosse, per un proprio tornaconto, fraudolentemente aggirato dall'autore della condotta illecita.

Il rischio riconducibile alla mancanza di validità, alla sospensione o revoca del permesso di soggiorno non è attuabile in quanto il Sistema di controllo informatizzato non consente di regolarizzare una posizione lavorativa irregolare.

Controlli esistenti

In considerazione della magnitudo del rischio con livello di esposizione medio e con un residuale impatto in termini di ricadute e pericolosità, si ritiene opportuno convalidare l'attuale sistema dei controlli.

14.4 – Misure e Procedure

Si ritiene opportuno integrare l'attuale sistema dei controlli con azioni specifiche di monitoraggio e *auditing* a cura dell'O.d.V. (attuate anche nell'ambito dei controlli previsti dal Sistema di Gestione per la Qualità). Le misure dovranno essere attivate al fine di prevenire l'utilizzo di manodopera senza permesso di soggiorno valido. Tali processi devono risultare adeguatamente formalizzati e dovranno essere periodicamente sottoposti a monitoraggio da parte dell'Organismo di Vigilanza.

L'Organismo di Vigilanza, acquisendo informazioni direttamente dalle Filiali e degli *audit* condotti presso le Filiali, effettua controlli sulla posizione contrattuale di dipendenti stranieri. A tal fine all'Organismo e agli *auditor* incaricati viene garantito libero accesso a tutta la documentazione di Filiale. Inoltre, l'Organismo di Vigilanza può attivarsi con specifici controlli a seguito delle segnalazioni ricevute, secondo quanto riportato nella Parte Generale del Modello 231.

Sulla base dei rischi rilevati si stabiliscono specifiche azioni preventive, le tempistiche, gli strumenti/risorse e le relative responsabilità.

Casistica	Responsabile	Descrizione attività di controllo, risorse, strumenti
1	O.d.V.	Formazione/informazione specifica per il personale
1	O.d.V./*auditor* incaricato	Prevedere che si effettuino controlli (registrati):
1	O.d.V.	Organizzazione di canali d'informazione tra O.d.V. e parti interessate su casi ritenuti a rischio in applicazione della Procedura PRT 03 - Protocollo segnalazioni di illeciti e irregolarità
1	O.d.V.	L'O.d.V. deve acquisire informazioni in merito all'efficacia delle azioni adottate, eventualmente prescrivere azioni integrative e informare il vertice aziendale.
1	O.d.V.	Redazione di Piano Annuale e consuntivo su Relazione Finale (§ 7 Parte Generale)

CAPITOLO 15: Reato di razzismo e xenofobia

15.1 – Principali Riferimenti Normativi

- "Art. 25-terdecies – (Razzismo e xenofobia);
- articolo 3, comma 3-bis, della legge 13 ottobre 1975, n. 654.

15.2 – Analisi iniziale

La Legge Europea 2017 ha previsto l'introduzione dell'art. 25 terdecies nel D. Lgs. 231/2001 rubricato Xenofobia e Razzismo elevando a reato presupposto della Responsabilità Amministrativa degli Enti il reato di cui all'articolo 3, comma 3-bis, della legge 13 ottobre 1975, n. 654 con ciò mirando a punire i partecipanti di organizzazioni, associazioni, movimenti o gruppi aventi tra i propri scopi l'incitamento alla discriminazione o alla violenza per motivi razziali, etnici, nazionali o religiosi, nonché la propaganda ovvero l'istigazione e l'incitamento, commessi in modo che derivi concreto pericolo di diffusione, fondati in tutto o in parte sulla negazione, sulla minimizzazione in modo grave o sull'apologia della Shoah o dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra. La disposizione è entrata in vigore il 12 Dicembre 2017; ma a seguito dell'emanazione del recentissimo D.lgs. 21/2018 siamo costretti a tornare a parlare del medesimo reato.

Se da un lato l'art. 25 terdecies è stato introdotto al fine di conferire rilevanza 231 al reato di cui all'art. 3, comma 3 bis L. 654/75, dall'altro lato il 6 Aprile 2018 è entrato in vigore il D.lgs. 21/2018 (Disposizioni di attuazione del principio di delega della riserva di codice nella materia penale a norma dell'articolo 1, comma 85, lettera q), della legge 23 giugno 2017, n. 103) che -all'art. 7, comma 1 lettera c) - ha abrogato l'art. 3 L. 654/75, senza, tuttavia, intervenire direttamente sul D.Lgs. 231/2001.

15.3 – Valutazione del Rischio

Modalità e contesti di commissione del reato

L'unica fattispecie di casistica rilevante si riferisce a particolari richieste avanzate da parte di imprese Clienti in merito all'esclusione discriminatoria di candidati o personale in somministrazione.

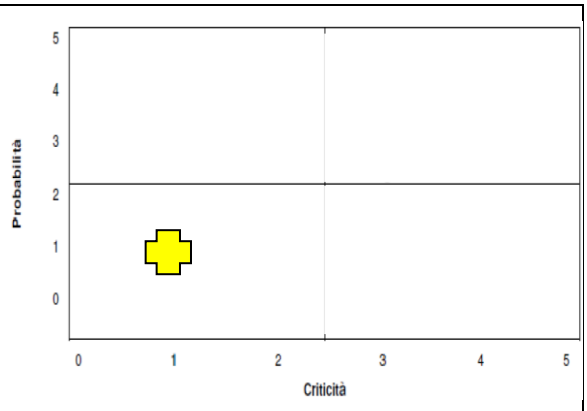
Controlli esistenti

In considerazione della bassa magnitudo del rischio non sono attive particolari azioni se non il controllo sul divieto tassativo di pubblicizzare, effettuare selezioni e predisporre contratti con elementi discriminatori di soggetti stranieri. L'aspetto è regolamentato anche all'interno delle procedure aziendali del Sistema Qualità.

Quantificazione del Rischio

Nell'ambito del reato si valuta la *magnitudo* sulla base delle variabili: probabilità e impatto e, in relazione al valore ottenuto e agli scostamenti, si definisce un piano operativo definendo le tipologie di misure preventive e di controllo da attuare.

Probabilità							
Molto alta	0,45	0,00	2,25	4,50	9,00	18,00	36,00
Alta	0,35	0,00	1,75	3,50	7,00	14,00	28,00
Media	0,25	0,00	1,25	2,50	5,00	10,00	20,00
Bassa	0,15	0,00	0,75	1,50	3,00	6,00	12,00
Molto bassa	0,05	0,00	0,25	0,50	1,00	2,00	4,00
Nulla	0,00	0,00	0,00	0,00	0,00	0,00	0,00
		0	5	10	20	40	80
		Nullo	Molto basso	Basso	Medio	Alto	Molto alto
		Impatto					



Probabilità	Impatto	Indice di Valutazione:
0,05	**5**	**0,25**

La Magnitudo si ottiene moltiplicando le variabili P e I (**M = P * I**); da cui ne deriva che l'Esposizione che può essere classificata **Bassa**, **Media** o **Elevata**. Strategie di *risk response*. Per un rischio alto: **evitare** il rischio (*risk avoidance*), per un rischio medio: **limitare** il rischio (*risk reduction*) o **trasferire** il rischio (*risk transferring/sharing*), per il rischio basso: **accettare** il rischio (*risk acceptance*).

15.4 – Misure e Procedure

Non si introduce nessuna ulteriore azione di controllo se non quella derivante dal divieto tassativo di azioni discriminatorie di soggetti stranieri e dalla normale ed efficace applicazione degli strumenti del Modello Organizzativo 231, vale a dire: Codice Etico e Regime Sanzionatorio e applicazione della Procedura PRT 03 - Protocollo segnalazioni di illeciti e irregolarità.

Schema riassuntivo di misure e procedure

Sulla base dei rischi rilevati si stabiliscono specifiche azioni preventive, le tempistiche, gli strumenti/risorse e le relative responsabilità.

Casistica	Responsabile	Descrizione attività di controllo, risorse, strumenti
1	Direzione	Condivisione Codice Etico e Regime Sanzionatorio.
1	O.d.V.	Organizzazione di canali d'informazione tra O.d.V. e parti interessate su casi ritenuti a rischio in applicazione della Procedura PRT 03 - Protocollo segnalazioni di illeciti e irregolarità
1	O.d.V.	L'O.d.V. deve acquisire informazioni in merito all'efficacia delle azioni adottate, eventualmente prescrivere azioni integrative e informare il vertice aziendale.
1	O.d.V.	Redazione di Piano Annuale e consuntivo su Relazione Finale (§ 7 Parte Generale)

CAPITOLO 16: Reato di tipo tributario

16.1 – Principali riferimenti normativi

Articoli di Legge	Cod.
Art. 25-quinquiesdecies	16.1
decreto-legge 26 ottobre 2019 n.124	16.2
Decreto Legislativo n. 74 del 2000	16.3
Decreto Legislativo 14/2019, Codice della crisi d'impresa	16.4
Decreto Legislativo 128 del 5 agosto 2015	16.5
Legge 4 ottobre 2019 n. 117	16.6
Direttiva Europea PIF	16.7
Decreto Legislativo n. 75 del 2020	16.8

16.2 – Analisi iniziale

La dichiarazione fraudolenta

Nella Gazzetta Ufficiale n. 252 del 26 ottobre 2019 è stato pubblicato il Decreto Legge 26 ottobre 2019, n. 124, recante "Disposizioni urgenti in materia fiscale e per esigenze indifferibili" (il "Decreto Fiscale"), che introduce il reato di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti nel catalogo dei reati presupposto rilevante al fine di configurare la responsabilità amministrativa delle persone giuridiche ai sensi del Decreto Legislativo n. 231.

L'art. 39, comma 2, del Decreto Fiscale introduce infatti nel Decreto 231 il nuovo articolo 25-quinquiesdecies, rubricato "Reati tributari", che dispone quanto segue: "In relazione alla commissione del delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dall'articolo 2 del decreto legislativo 10 marzo 2000, n. 74, si applica all'ente la sanzione pecuniaria fino a cinquecento quote".

Il reato di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti è previsto dall'art. 2 del Decreto Legislativo n. 74 del 2000, a norma del quale "E' punito con la reclusione da quattro a otto anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti per operazioni inesistenti, indica in una delle dichiarazioni annuali relative a dette imposte elementi passivi fittizi. Il fatto si considera commesso avvalendosi di fatture o altri documenti per operazioni inesistenti quando tali fatture o documenti sono registrati nelle scritture contabili obbligatorie, o sono detenuti a fine di prova nei confronti dell'amministrazione finanziaria". All'evidenza, si tratta di un reato di mera condotta, a consumazione istantanea, che si realizza nel momento in cui viene presentata la dichiarazione fiscale.

La predisposizione e la registrazione dei documenti attestanti le operazioni inesistenti sono condotte meramente preparatorie e non sono punibili, nemmeno a titolo di tentativo. Il reato è punito a titolo di dolo specifico, poiché è caratterizzato dalla finalità di evadere le imposte sui redditi o sul valore aggiunto (compresi il fine di conseguire un indebito rimborso o il riconoscimento di un inesistente credito d'imposta, per sé o per altri).

Si evidenzia che, secondo la definizione prevista dall'art. 1 D. Lgs. n. 74/2000, "per fatture per operazioni inesistenti si intendono le fatture o gli altri documenti aventi rilievo probatorio analogo in base alle norme tributarie, emessi a fronte di operazioni non realmente effettuate in tutto o in parte o che indicano i corrispettivi o l'imposta sul valore aggiunto in misura superiore a quella reale, ovvero che riferiscono l'operazione a soggetti diversi da quelli effettivi".

Frodi in materia di Iva tra i reati previsti dal Decreto Legislativo 231/2001

Nella Gazzetta Ufficiale n. 245 del 18 ottobre 2019 è stata pubblicata la Legge 4 ottobre 2019 n. 117, in vigore dal 2 novembre, con la delega al Governo per recepire la Direttiva (UE) 2017/1371 "relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale" ("Direttiva PIF" "Legge di delegazione europea 2018").

Ai sensi dell'art. 3, comma 1, lettera e), della Legge di delegazione europea 2018, nell'esercizio della delega per l'attuazione della Direttiva PIF, il Governo dovrà integrare le disposizioni del Decreto 231 prevedendo espressamente la responsabilità amministrativa da reato delle persone giuridiche anche per le "gravi" frodi in materia IVA, laddove il concetto di gravità è definito dalla Direttiva PIF avendo riguardo al carattere transfrontaliero delle condotte illecite (connessa a due o più Stati membri") e all'elevato ammontare del danno complessivo ("almeno pari a 10 milioni di €.").

Oltre alle sanzioni amministrative, il Governo dovrà introdurre nel Decreto 231 anche le sanzioni previste dall'articolo 9 della Direttiva PIF, che comprendono l'esclusione dal godimento di un beneficio o di un aiuto pubblico, l'esclusione temporanea o permanente dalle procedure di gara pubblica, l'interdizione temporanea o permanente di esercitare un'attività commerciale, l'assoggettamento a sorveglianza giudiziaria, l'applicazione di provvedimenti giudiziari di

scioglimento e la chiusura temporanea o permanente degli stabilimenti che sono stati usati per commettere il reato, con la precisazione che tutte le sanzioni dovranno essere “effettive, proporzionate e dissuasive”.

Per effetto della Legge 4 ottobre 2019 n. 117, in vigore dal 2 novembre, con la delega al Governo per recepire la Direttiva (UE) 2017/1371 relativa alla lotta contro la frode che lede gli interessi finanziari dell’Unione, è stato pubblicato il D.Lgs. 14 luglio 2020, n. 75, recante "Attuazione della direttiva (UE) 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale”, ossia il provvedimento normativo di recepimento della c.d. "Direttiva PIF”. Tra le modifiche introdotte, si segnala l’estensione della responsabilità degli enti per i delitti di gravi frodi IVA in ipotesi di dichiarazione infedele (art. 4 D.Lgs. n. 74/2000), omessa dichiarazione (art. 5) e indebita compensazione (art. 10-quater D.Lgs. n. 74/2000).

Per questa tipologia di reati, oltre alle sanzioni amministrative, le sanzioni che comprendono l’esclusione dal godimento di un beneficio o di un aiuto pubblico, l’esclusione temporanea o permanente dalle procedure di gara pubblica, l’interdizione temporanea o permanente di esercitare un’attività commerciale, l’assoggettamento a sorveglianza giudiziaria, l’applicazione di provvedimenti giudiziari di scioglimento e la chiusura temporanea o permanente degli stabilimenti che sono stati usati per commettere il reato, con la precisazione che tutte le sanzioni dovranno essere “effettive, proporzionate e dissuasive”.

A titolo esemplificativo, possiamo elencare alcune condotte riconducibili a reati tributari rilevanti ai fini 231:

I) Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2, D.Lgs. 74/2000):una società emette fatture per prestazioni mai eseguite e in sede di dichiarazione IVA le inserisce tra gli elementi contabili, ottenendo così un risparmio fraudolento per la società.

II) Dichiarazione fraudolenta mediante altri artifici (art. 3, D.Lgs. n. 74/2000): una società si avvale di documenti falsi al fine di evadere l’imposta sui redditi, ottenendo così un risparmio fraudolento per la società.

III) Emissione di fatture per operazioni inesistenti (art. 8, D.Lgs. n. 74/2000):la società emette fattura per operazioni inesistenti, al fine di consentire ad un terzo di evadere le imposte sui redditi o sul valore aggiunto.

IV) Occultamento o distruzione di documenti e sottrazione al pagamento (art. 10, D.Lgs. 74/2000): la società distrugge materialmente le scritture contabili obbligatorie, con impossibilità di ricostruzione del volume di affari, al fine di evadere le imposte ed ottenere un risparmio fraudolento per la società.

V) Sottrazione fraudolenta al pagamento di imposte (art. 11, D.Lgs. 74/2000):un amministratore disperde beni della società per sottrarla al pagamento delle imposte, ottenendo un risparmio fraudolento per la società.

VI) Dichiarazione infedele (limitatamente all’ambito di sistemi fraudolenti transfrontalieri, al fine di evadere l’IVA, per un importo complessivo non inferiore a 10 milioni di euro) (art. 4, D.Lgs. 74/2000): l’ente, al fine di evadere l’imposta sul valore aggiunto, falsifica la relativa dichiarazione, superando i limiti indicati dal legislatore ed ottenendo un risparmio fraudolento per l’ente stesso.

VII) Omessa dichiarazione (limitatamente all’ambito di sistemi fraudolenti transfrontalieri, al fine di evadere l’IVA, per un importo complessivo non inferiore a 10 milioni di euro) (art. 5, D.Lgs. 74/2000):l’ente, al fine di evadere l’imposta sul valore aggiunto, non presenta la relativa dichiarazione, superando i limiti indicati dal legislatore ed ottenendo un risparmio fraudolento per l’ente stesso.

VI) Indebita compensazione (limitatamente all’ambito di sistemi fraudolenti transfrontalieri, al fine di evadere l’IVA, per un importo complessivo non inferiore a 10 milioni di euro) (art. 10-quater, D.Lgs. 74/2000): l’ente, mediante il supporto di documentazione falsa, prospetta una compensazione fondata su un credito inesistente o non spettante, superando i limiti indicati dal legislatore ed ottenendo un vantaggio fraudolento per l’ente stesso

Da un punto di vista operativo, Etjca S.p.A. deve effettuare una propria auto-analisi interna e valutare se le fattispecie tributarie introdotte siano rilevanti o meno, con riferimento alle specifiche attività svolte. In questo senso, si dovrà procedere attraverso: i) la valutazione del rischio di reato nell’ambito dei processi aziendali; ii) la valutazione dell’efficacia dei presidi già esistenti per la riduzione del rischio, e quindi l’identificazione delle eventuali carenze o ambiti di miglioramento; iii) l’introduzione di eventuali ulteriori presidi atti a contenere il c.d. rischio residuo.

La matrice seguente identifica le aree (funzioni e processi) oggetto di indagine in riferimento ai rischi specifici.

Funzioni/Aree	Processi, fasi e attività	Casistica
Amministrazione	Processo contabile/amministrativo	1

Processo **Processi finanziari**				Giudizio Preliminare [2]	Controlli Esistenti						Valutazione Controlli [3]	Ruolo della Funzione					
Sigla Area/Funz.	N. Fase/Attività	Cod. Reato	Fattore [1]		Esistenza di Procedure	Aggiornamento Procedure	Esistenza di Deleghe	Conoscenza e Comunicazione	Suddivisione Compiti	Controlli e Monitoraggi		Operativo	Decisionale	Autorizzativo	Monitoraggio	Sanzionatorio	*Training*
AMM	1	16	I, E, D	B	☒	☒	☑	☑	☑	☑	E	☑	☑	☑	☑	☒	☒
RU	2	16	I, E, D	B	☑	☑	☑	☑	☑	☑	E	☑	☑	☒	☑	☒	☒
CLI	3	16	I, E, D	M	☑	☑	☑	☑	☑	☑	M	☑	☑	☒	☑	☒	☒

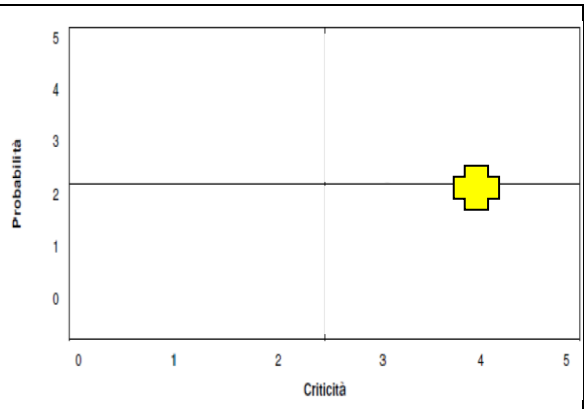
1 I = Interno, E = Esterno, D = Decisionale. **2** Giudizio preliminare rischio reato: A = Alto, M = Medio, B = Basso, I = Inesistente. **3** Valutazione efficacia e adeguatezza dei controlli: I = Inefficaci, M = da migliorare, E = Efficaci, N = Non Esistenti. 4 ☒ = Elemento non presente; ☑ = Elemento Presente.

Annotazioni. L'analisi iniziale indica che l'entità del rischio è da considerarsi di media entità.

16.3 – Valutazione del Rischio

Nell'ambito dei singoli rischi di reato, potenzialmente attivi in ognuna delle aree aziendali analizzate, se ne valuta la *magnitudo* di ognuno di essi sulla base delle variabili: probabilità e impatto e, sulla base del valore ottenuto e degli scostamenti, si definisce un piano operativo definendo innanzitutto le tipologie di misure preventive e di controllo da attuare .

Probabilità		0,00	2,25	4,50	9,00	18,00	36,00
Molto alta	0,45						
Alta	0,35	0,00	1,75	3,50	7,00	14,00	28,00
Media	0,25	0,00	1,25	2,50	5,00	10,00	20,00
Bassa	0,15	0,00	0,75	1,50	3,00	6,00	12,00
Molto bassa	0,05	0,00	0,25	0,50	1,00	2,00	4,00
Nulla	0,00	0,00	0,00	0,00	0,00	0,00	0,00
		0	5	10	20	40	80
		Nullo	Molto basso	Basso	Medio	Alto	Molto alto
		Impatto					



Probabilità	Impatto	Indice di Valutazione:
0,15	**40**	**6**

La Magnitudo si ottiene moltiplicando le variabili P e I (**M = P * I**); da cui ne deriva che l'Esposizione che può essere classificata **Bassa**, **Media** o **Elevata**. Strategie di *risk response*. Per un rischio alto: **evitare** il rischio (*risk avoidance*), per un rischio medio: **limitare** il rischio (*risk reduction*) o **trasferire** il rischio (*risk transferring/sharing*), per il rischio basso: **accettare** il rischio (*risk acceptance*).

Annotazioni sulla valutazione e modalità e contesti di commissione del reato

Il ciclo attivo e passivo, o anche la *supply chain*, sono comuni a tutte le imprese e anche in strutture medio-grandi sono molteplici sia i centri di acquisto, cioè soggetti che sono abilitati ad acquistare beni e servizi per l'impresa sia i centri dai quali pervengono all'impresa dati e informazioni per la fatturazione attiva.

In entrambi i casi, nelle dinamiche della stessa, potrebbero originarsi fatture false passive o attive.

La prassi dimostra che numerose fattispecie risultano particolarmente insidiose da rilevare, in particolare quando entrano in gioco rapporti con soggetti esteri. Non da ultimo, processi di digitalizzazione non sufficientemente adeguati hanno finito per favorire il fenomeno.

Ora, la prima linea di difesa per prevenire questa tipologia di reati è sicuramente l'adozione di un sistema amministrativo – contabile adeguato, che dovrebbe essere affiancato da un sistema gestionale altrettanto efficace

(nella fattispecie controllo di gestione di ETJCA S.p.A.). Le "distrazioni" contabili e gestionali, cioè la scarsa attenzione dell'impresa a questi aspetti sono terreno fertile per la commissione dei reati in argomento.

Si segnala peraltro che il decreto legislativo 14/2019, Codice della crisi d'impresa, già prescrive l'adozione di un adeguato assetto amministrativo-contabile volto a rilevare tempestivamente eventuali crisi di impresa ad un numero di soggetti addirittura maggiore rispetto a coloro che hanno introdotto i Modelli 231. Ai fini della prevenzione del reato in argomento non deve essere adottato un assetto amministrativo-contabile ulteriore o nuovo, ma le esigenze e le finalità, pur in apparenza diverse, coincidono per numerosi aspetti. Dovrebbe semmai trattarsi di valutare l'adozione di qualche funzionalità gestionale e/o contabile, ma sempre nell'ambito dello stesso assetto amministrativo - contabile. Un buon sistema gestionale e contabile è sicuramente una misura necessaria, ma può non essere sufficiente ai fini di un'efficace prevenzione.

Per le società di grandi dimensioni l'ingresso nel regime di adempimento collaborativo di cui al decreto legislativo n.128 del 5 agosto 2015, con il relativo obbligo di rilevare, misurare e monitorare il rischio fiscale, può essere sicuramente una strada percorribile efficace.

Il presidio del rischio fiscale nell'ambito del Modello 231 prevede strumenti atti a prevenire il reato di falsa fatturazione. Le misure preventive dovrebbero consistere sempre nella creazione al proprio interno di un presidio del rischio fiscale. In linea generale, il presidio del rischio fiscale si estrinseca anzitutto in un preventivo "*risk assessment*" idoneo a individuare e comprendere i processi e l'organizzazione interni, segnalarne eventuali debolezze e suggerire nel contempo misure correttive, il tutto in un'ottica fiscale.

Da altra prospettiva, si tratta di migliorare la *corporate governance* in ambito fiscale, o come ormai si dice, di migliorare la *tax governance* dell'impresa, per la quale occorre sia conoscenza delle principali regole di governo societario sia della materia tributaria.

16.4 – Misure e Procedure

In generale, si deve considerare che si tratta di reati "trasversali", nel senso che, oltre ad interessare in via diretta l'area fiscale e l'area amministrativa contabile, hanno riflessi anche su altre aree e processi aziendali.

Con riferimento ai reati di natura dichiarativa, si dovrà considerare che si realizzano con la presentazione delle dichiarazioni volte a determinare la base imponibile e l'imposta IRES ed IVA, con gli antecedenti necessari nelle attività relative alla redazione dei bilanci ed alla registrazione contabile di fatture o altri documenti e quindi avendo come riferimento il ciclo passivo dell'azienda.

Con riferimento agli ulteriori reati di natura non dichiarativa, assume rilievo il ciclo attivo dell'azienda, dovendo qui fare riferimento all'emissione di fatture o altri documenti a fronte di operazioni inesistenti a fine di consentire a terzi l'evasione fiscale.

Con riferimento poi all'occultamento e distruzione di documenti e sottrazione al pagamento di imposte, si dovrà fare attenzione anche ai sistemi di sicurezza nell'archiviazione cartacea o informatica, tali da escludere condotte rilevanti, nonché alla 'gestione' del patrimonio.

Il Sistema in atto in ETJCA prevede una procedura di controllo della fatturazione attiva e passiva che prevede il coinvolgimento di più soggetti e quindi un sistema reciproco autocontrollo e regolazione.

Per la ricezione e gestione delle fatture passive, si parte dalla richiesta interna del Dirigente interessato, la successiva emissione dell'ordine con controllo preventivo da parte del Responsabile AMM, il ricevimento fattura, la ricerca dell'ordine (uff. fornitori), registrazione e pagamento da tesoreria (autorizzato da AMM via bancaria).

Per la produzione delle fatture attive si parte dalla richiesta del dirigente interessato e il conseguente inoltro della fattura da parte dell'Ufficio AMM.

Si fa presente non che esiste fatturazione attiva e passiva con l'estero.

A livello consuntivo si attuano controlli, su più livelli, derivanti dalla approvazione e successiva certificazione del bilancio, controlli sulle periodiche dichiarazioni IVA e controlli preliminari alla dichiarazione dei redditi d'impresa; i controlli sono eseguiti a livello di AMM, a livello di C.d.A. e quindi il Collegio dei Sindaci, di Società di Revisione e, in ultima istanza, di O.d.V.

Sulla base dei rischi rilevati si stabiliscono specifiche azioni preventive, le tempistiche, gli strumenti/risorse e le relative responsabilità.

Casistica	Responsabile	Descrizione attività di controllo, risorse, strumenti
1	Amministrazione	Gestione corretta del processo di fatturazione attiva, con identificazione di ruoli e segregazione delle funzioni coinvolte nel processo e monitoraggio. Controllo delle situazioni anomale nelle condizioni di pagamento accordate e dell'incasso del credito derivante dalla prestazione effettuata
1	Amministrazione Studio Fiscale	Registrazione di ogni operazione economico finanziaria nel rispetto dei principi, criteri, modalità di redazione, tenuta e conservazione della contabilità dettate dalla normativa vigente
1	Amministrazione Studio Fiscale	Corretto calcolo delle imposte e conseguente presentazione di dichiarazioni e/o documenti fiscali previsti e assolvimento di ogni onere;
1	Amministrazione Studio Fiscale	Corretto calcolo degli adempimenti connessi alle imposte sui redditi e IVA per assicurare la tracciabilità delle attività. Separazione dei ruoli e verifiche incrociate.
1	Amministrazione	Definizione e aggiornamento della lista di fornitori attuali e potenziali per ogni tipologia di acquisto o categoria merceologica. Definizione dei criteri di selezione dei fornitori e indicazione dei criteri di valutazione delle offerte ricevute dagli stessi. Verificare la corrispondenza tra la denominazione/ragione sociale del fornitore e l'intestazione del conto corrente, e verifica delle richieste dei fornitori relative a pagamenti da effettuarsi su istituti bancari situati in specifici Paesi (a fiscalità privilegiata o comunque diversi da quelli di stabilimento dei fornitori medesimi). Per tutti: definizione delle modalità di presentazione delle offerte e formalizzazione degli accordi con il fornitore selezionato previa firma del Modello Clausole Contrattuali.
1	Amministrazione	Gestione degli acquisti di beni e servizi, anche distinguendo le diverse tipologie (beni, servizi, investimenti, piccoli acquisti ricorrenti di modesto importo, ecc.), con identificazione di ruoli e responsabilità. Separazione dei ruoli in particolare tra la gestione dell'ordine, la gestione dei pagamenti e la registrazione delle spese. Procedura di verifica della corrispondenza tra gli importi previsti nell'ordine di acquisto e quelli indicati in fattura, con previsione delle modalità di gestione e relative approvazioni per eventuali modifiche/integrazioni degli ordini di acquisto.
1	Amministrazione	Applicare specifica regolamentazione per la gestione degli ordinativi. Per acquisti inferiori a 5000 euro è prevista la firma del Direttore Per acquisti superiori a 5000 euro è prevista l'autorizzazione dell'AU.
1	Amministrazione	Verifica e controllo, prima del pagamento della fattura, del contenuto della fattura, dell'ordine e dell'attestazione sul bene/servizio ricevuto. Controllo, attraverso sistemi informatici aziendali, al fine di evitare la duplice registrazione della fattura e dei pagamenti.
1	Amministrazione	Previsione di un'autorizzazione specifica alla trasferta di un dipendente e dell'approvazione della nota spese da parte del supervisore, con fissazione di limiti da rispettare per le diverse tipologie di spesa definiti ed in generale, previsione di specifiche spese rimborsabili con monitoraggio su rimborsi o spese di valore eccessivo/ricorrente e utilizzo di carte di credito aziendali, per minimizzare o escludere la gestione del contante da parte dei dipendenti e divieto di ritirare contanti con le carte di credito aziendali
1	O.d.V. e AU	Pianificazione e attuazione di programmi di *audit* di primo e secondo livello.
1	O.d.V.	Condivisione Codice di Comportamento e Regolamento Sanzionatorio.
1	O.d.V.	Costante attività formativa, a tutti i destinatari, su quanto previsto dal Codice etico e dal Modello organizzativo 231 aziendale, assicurando diffusione/formazione sulle diverse procedure/protocolli;
1	O.d.V.	L'O.d.V. deve acquisire informazioni in merito all'efficacia delle azioni adottate, eventualmente prescrivere azioni integrative e informare il vertice aziendale.
1	O.d.V. e AU	Redazione di Relazione Annuale O.d.V. e Programma Annuale *Compliance*.

CAPITOLO 17: Frode in competizioni sportive ed esercizio abusivo di gioco o scommesse e giochi d'azzardo

17.1 – Principali riferimenti normativi

Articoli di Legge	Cod.
Art. 25-quaterdecies – Frode in competizioni sportive, esercizio di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati	17.1
Legge 3 maggio 2019, n. 39	17.2
Artt. 1 e 4, della legge 13 dicembre 1989, n. 401	17.3

17.2 – Analisi iniziale

Con la Legge 3 maggio 2019 n. 39, recante la "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulle manipolazioni sportive" il tema della responsabilità amministrativa degli enti è entrato in modo dirompente nel mondo dello sport. La citata normativa, recependo le direttive europee, ha provveduto a inserire alcuni nuovi reati nell'elenco del D.Lgs. 231/01 al fine di prevenire la commissione di illeciti in ambito sportivo.

A tal fine sono dunque è stato ampliato il catalogo delle condotte illecite rilevanti D. Lgs. ex 231/01, sia in relazione all'organizzazione di giochi e scommesse e sia inserendo quali reati presupposto, il delitto di frode sportiva.

Con particolare riferimento a quest'ultima novità, si tratta di una previsione normativa sostanzialmente diretta alle società sportive, e in particolar modo a quelle professionistiche, che dunque aprirsi un nuovo fronte di possibili sanzioni da parte dell'ordinamento per la condotta illecita del proprio management.

La Legge 3 maggio 2019, n. 39 ha quindi introdotto nel D.Lgs. 231/2001 il nuovo art. 25 quaterdecies, che integra la lista dei reati presupposto con i reati di frode in competizioni sportive e di esercizio abusivo di attività di giuoco o di scommesse. Nello specifico, il delitto di frode sportiva (art. 1 L. 401/1989) incrimina "chiunque offre o promette denaro o altra utilità o vantaggio a taluno dei partecipanti ad una competizione sportiva organizzata dalle federazioni riconosciute, al fine di raggiungere un risultato diverso da quello conseguente al corretto e leale svolgimento della competizione, ovvero compie altri atti fraudolenti volti al medesimo scopo" nonché "il partecipante alla competizione che accetta il denaro o altra utilità o vantaggio, o ne accoglie la promessa".

L'art. 4 dello stesso articolato normativo contempla, invece, diverse fattispecie connesse all'esercizio, organizzazione, vendita di attività di giochi e scommesse in violazione di autorizzazioni o concessioni amministrative.

La matrice seguente identifica le aree aziendali (funzioni e processi) oggetto di indagine in riferimento ai rischi specifici.

Funzioni/Aree	Processi, fasi e attività	Casistica
Amministrazione	Stipula contratti di sponsorizzazione	1
Marketing	Stipula contratti di sponsorizzazione	1

Processo **Processi finanziari**				Giudizio Preliminare [2]	Controlli Esistenti						Valutazione Controlli [3]	Ruolo della Funzione					
Sigla Area/Funz.	N. Fase/Attività	Cod. Reato	Fattore [1]		Esistenza di Procedure	Aggiornamento Procedure	Esistenza di Deleghe	Conoscenza e Comunicazione	Suddivisione Compiti	Controlli e Monitoraggi		Operativo	Decisionale	Autorizzativo	Monitoraggio	Sanzionatorio	*Training*
AMM	1	17	I, E	B	☒	☒	☑	☑	☑	☑	E	☑	☑	☑	☑	☒	☒
MKT	2	17	I, E	B	☑	☑	☑	☑	☑	☑	E	☑	☑	☒	☑	☒	☒

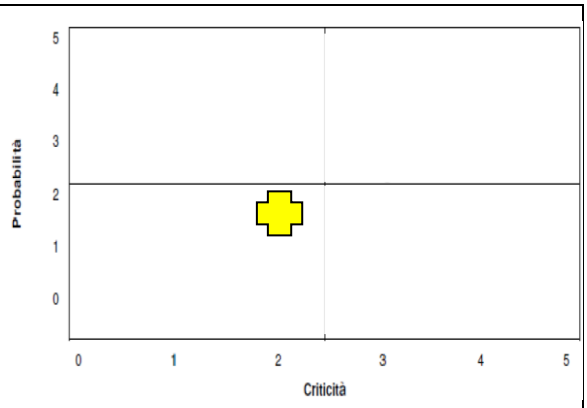
1 I = Interno, E = Esterno, D = Decisionale. **2** Giudizio preliminare rischio reato: A = Alto, M = Medio, B = Basso, I = Inesistente. **3** Valutazione efficacia e adeguatezza dei controlli: I = Inefficaci, M = da migliorare, E = Efficaci, N = Non Esistenti. 4 ☒ = Elemento non presente; ☑ = Elemento Presente.

Annotazioni. L'analisi iniziale indica che l'entità del rischio è da considerarsi bassa in quanto non esiste situazione e contratto che possa portare vantaggi e interessi nel compimento di questa fattispecie di reato. Esiste tuttavia un basso rischio a seguito di problematiche legate alla sottoscrizione di contratti di sponsorizzazione.

17.3 – Valutazione del Rischio

Nell'ambito dei singoli rischi di reato, potenzialmente attivi in ognuna delle aree aziendali analizzate, se ne valuta la *magnitudo* di ognuno di essi sulla base delle variabili: probabilità e impatto e, sulla base del valore ottenuto e degli scostamenti, si definisce un piano operativo definendo innanzitutto le tipologie di misure preventive e di controllo da attuare.

Probabilità							
Molto alta	0,45	0,00	2,25	4,50	9,00	18,00	36,00
Alta	0,35	0,00	1,75	3,50	7,00	14,00	28,00
Media	0,25	0,00	1,25	2,50	5,00	10,00	20,00
Bassa	0,15	0,00	0,75	1,50	3,00	6,00	12,00
Molto bassa	0,05	0,00	0,25	0,50	1,00	2,00	4,00
Nulla	0,00	0,00	0,00	0,00	0,00	0,00	0,00
		0	5	10	20	40	80
		Nullo	Molto basso	Basso	Medio	Alto	Molto alto
		Impatto					



Probabilità	Impatto	Indice di Valutazione:
0,15	**10**	**1,5**

La Magnitudo si ottiene moltiplicando le variabili P e I (**M = P * I**); da cui ne deriva che l'Esposizione che può essere classificata **Bassa**, **Media** o **Elevata**. Strategie di *risk response*. Per un rischio alto: **evitare** il rischio (*risk avoidance*), per un rischio medio: **limitare** il rischio (*risk reduction*) o **trasferire** il rischio (*risk transferring/sharing*), per il rischio basso: **accettare** il rischio (*risk acceptance*).

Annotazioni sulla valutazione.

Per quanto riguarda il reato di frode sportiva nella sua forma più classica, e cioè quella consistente nel richiedere a un partecipante a una competizione sportiva di limitare il proprio impegno agonistico a fronte di una somma di denaro o di qualsiasi altra utilità, al fine di raggiungere un risultato diverso da quello conseguente al leale e corretto svolgimento della competizione, il modello di gestione dovrà, tra le altre cose, prevedere regole interne atte a controllare la gestione delle risorse finanziare, secondo dinamiche che possono in qualche modo richiamare i protocolli di gestione aziendale utilizzati al fine di prevenire reati di corruzione, delitto che per quanto riguarda la prospettiva 231/01 presenta alcune analogie con la frode sportiva (vedere al riguardo quanto già riscritto al § 13: Reato di corruzione tra privati).

Più problematica in tema di prevenzione di future condotte illecite in ambito sportivo appare invece la locuzione prevista all'art. 1 della L. 409/81, laddove si fa riferimento a "altri atti fraudolenti volti al medesimo scopo" (vale a dire il raggiungimento di un risultato "viziato"): si tratta di una formulazione di carattere generico, (a forma libera, per usare il termine tecnico) che lascia aperta la porta della rilevanza penale a una serie indefinita di condotte, al limite dell'atipicità. Per comprendere l'ampio ambito della previsione criminosa, è forse utile ricordare che, nell'esperienza giurisprudenziale, sono stati ritenute quali condotte costituente frode sportiva comportamenti del tutto diversi quali la somministrazione di sostanze per alterare prestazioni sportive (per di più in concorso con gli specifici reati in tema di doping) ma anche condotte volte ad ottenere designazioni arbitrali gradite in violazione dei regolamenti federali di riferimento. Tuttavia, le fattispecie appena descritte non sono riconducibili alle normali attività di ETJCA.

Dunque, la condotta del dirigente della società sportiva che si adoperi per alterare illecitamente l'esito della competizione non si limiterà ad avere per l'ente di appartenenza riflessi sanzionatori unicamente nell'ambito del processo sportivo ma con il nuovo art. 25 quaterdecies D. Lgs. 231/01 anche il club avvantaggiato dall'illecito può essere in astratto direttamente passibile di gravi sanzioni di natura amministrativa irrogate dal giudice penale, che possono consistere di una pena pecuniaria commisurata alle sue condizioni economiche e patrimoniali, ma, soprattutto, anche a sanzioni di natura interdittiva, in astratto anche molto invasive, che ne possono limitare in modo sensibile l'operatività, quali l'interdizione dall'esercizio dell'attività.

Modalità e contesti di commissione del reato

Per quanto riguarda ETJCA si rileva un'unica residuale fattispecie che si colloca nell'ambito della stipula di contratti di sponsorizzazione a opera dell'Ufficio Marketing.

In un contesto di sponsorizzazione sportiva ETJCA stipula diversi contratti di sponsorizzazione con diversi soggetti legati al CONI; in questo contesto il Sistema 231/01 deve poter prevenire situazioni di correità (in concorso con società sportive) o situazioni di corruzione, direttamente perpetrata da soggetti facenti capo a ETJCA, finalizzate ad avvantaggiare il *brand* mediante la pubblicizzazione o sponsorizzazione di società sportive. Si consideri, per esempio, il caso in cui si corrompessero uno o più giocatori di una squadra sportiva avversaria allo scopo di incrementare illecitamente la visibilità mediatica da sponsorizzazione derivante da un elevato numero di vittorie in un trofeo a eliminazione diretta.

17.4 – Misure e Procedure

Il Sistema in atto in ETJCA prevede una procedura di controllo della stipula dei contratti di sponsorizzazione e della successiva fatturazione passiva che prevede il coinvolgimento di più soggetti e quindi un sistema reciproco autocontrollo e regolazione. Per la approvazione di un contratto di sponsorizzazione e successiva ricezione e gestione delle fatture passive, si parte dalla richiesta interna del Dirigente interessato, la successiva emissione dell'ordine con controllo preventivo da parte del Responsabile AMM, il ricevimento fattura, la ricerca dell'ordine (uff. fornitori), registrazione e pagamento da tesoreria (autorizzato da AMM via bancaria).

Si applicano infine i seguenti strumenti tipici del Modello di prevenzione 231/01 di ETJCA S.p.A.:

Casistica	Responsabile	Descrizione attività di controllo, risorse, strumenti
1	Direzione	Condivisione Codice Etico e Regime Sanzionatorio.
1	O.d.V.	Organizzazione di canali d'informazione tra O.d.V. e parti interessate su casi ritenuti a rischio in applicazione della Procedura PRT 03 - Protocollo segnalazioni di illeciti e irregolarità
1	O.d.V.	L'O.d.V. deve acquisire informazioni in merito all'efficacia delle azioni adottate, eventualmente prescrivere azioni integrative e informare il vertice aziendale.
1	O.d.V.	Redazione di Piano Annuale e consuntivo su Relazione Finale (§ 7 Parte Generale)

CAPITOLO 18: Reato di Contrabbando

18.1 – Principali riferimenti normativi

Articoli di Legge	Cod.
25 sexdecies (Contrabbando)	18.1
D.Lgs. 75/2020	18.2
DPR 43/1973	18.3

18.2 – Analisi iniziale

La matrice seguente identifica le aree aziendali (funzioni e processi) oggetto di indagine in riferimento ai rischi specifici.

Funzioni/Aree	Processi, fasi e attività	Casistica
Nessuna	Nessun processo	/

Processo				Giudizio Preliminare [2]	Controlli Esistenti						Valutazione Controlli [3]	Ruolo della Funzione					
Sigla Area/Funz.	N. Fase/Attività	Cod. Reato	Fattore [1]		Esistenza di Procedure	Aggiornamento Procedure	Esistenza di Deleghe	Conoscenza e Comunicazione	Suddivisione Compiti	Controlli e Monitoraggi		Operativo	Decisionale	Autorizzativo	Monitoraggio	Sanzionatorio	*Training*
/	/	18	I	I	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒

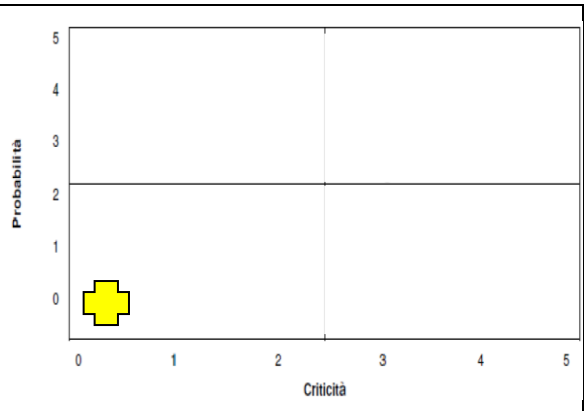
1 I = Interno, E = Esterno, D = Decisionale. **2** Giudizio preliminare rischio reato: A = Alto, M = Medio, B = Basso, I = Inesistente. **3** Valutazione efficacia e adeguatezza dei controlli: I = Inefficaci, M = da migliorare, E = Efficaci, N = Non Esistenti. 4 ☒ = Elemento non presente; ☑ = Elemento Presente.

Annotazioni. Si considerino praticamente nulli i rischi di commissione reato di contrabbando in quanto i servizi erogati da Etjca S.p.A. non contemplano attività che possano ricondurre a tali fattispecie di reati. Non esistono estremi per rilevare rischi residui e di conseguenza non esistono procedure e controlli specifici.

18.3 – Valutazione del Rischio

Nell'ambito dei singoli rischi di reato, potenzialmente attivi ognuna delle aree aziendali analizzate, se ne valuta la *magnitudo* di ognuno di essi sulla base delle variabili: probabilità e impatto e, sulla base del valore ottenuto e degli scostamenti, si definisce un piano operativo definendo innanzitutto le tipologie di misure preventive e di controllo da attuare.

Probabilità							
Molto alta	0,45	0,00	2,25	4,50	9,00	18,00	36,00
Alta	0,35	0,00	1,75	3,50	7,00	14,00	28,00
Media	0,25	0,00	1,25	2,50	5,00	10,00	20,00
Bassa	0,15	0,00	0,75	1,50	3,00	6,00	12,00
Molto bassa	0,05	0,00	0,25	0,50	1,00	2,00	4,00
Nulla	0,00	0,00	0,00	0,00	0,00	0,00	0,00
		0	5	10	20	40	80
		Nullo	Molto basso	Basso	Medio	Alto	Molto alto
		Impatto					



Probabilità	Impatto	Indice di Valutazione:
0	**0**	**0**

La Magnitudo si ottiene moltiplicando le variabili P e I (**M = P * I**); da cui ne deriva che l'Esposizione che può essere classificata **Bassa**, **Media** o **Elevata**. Strategie di *risk response*. Per un rischio alto: **evitare** il rischio (*risk avoidance*), per un rischio medio: **limitare** il rischio (*risk reduction*) o **trasferire** il rischio (*risk transferring/sharing*), per il rischio basso: **accettare** il rischio (*risk acceptance*).

Annotazioni sulla valutazione. Non esistono processi a rischio e, di conseguenza, non si attivano controlli specifici.

18.4 – Misure e Procedure

Sulla base dei rischi rilevati si decide di non approvare specifiche azioni preventive.

Casistica	Responsabile	Descrizione attività di controllo, risorse, strumenti
/	/	/