ITALCER GROUP

DESIGN SURFACES

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

Sintesi del MOGC di Italcer S.p.A. SB
Sua implementazione e funzionamento

Revisione del 31.03.25

ELIOS ceramica · CERAMICA Rondine · BOTTEGA · LA FABBRICA AVA EXTRAORDINARY TILES · AVASTONE · SPRAY DRY

Premessa

Il 14 dicembre 2021 il Consiglio di Amministrazione di Italcer S.p.A. SB («**Italcer**» o la «**Società**») ha approvato l'adozione del Modello di Organizzazione, Gestione e Controllo (di seguito anche «Modello Organizzativo» o «MOGC») ai sensi del D. Lgs. 231/2001.
Nella stessa sede, veniva nominato l'Organismo di Vigilanza (di seguito anche «**OdV**») in composizione collegiale, le cui attività sono guidate dal Regolamento dell'Organismo di Vigilanza. Annualmente l'OdV redige e presenta al Consiglio di Amministrazione una relazione sull'attività svolta e un piano di audit per l'anno successivo.

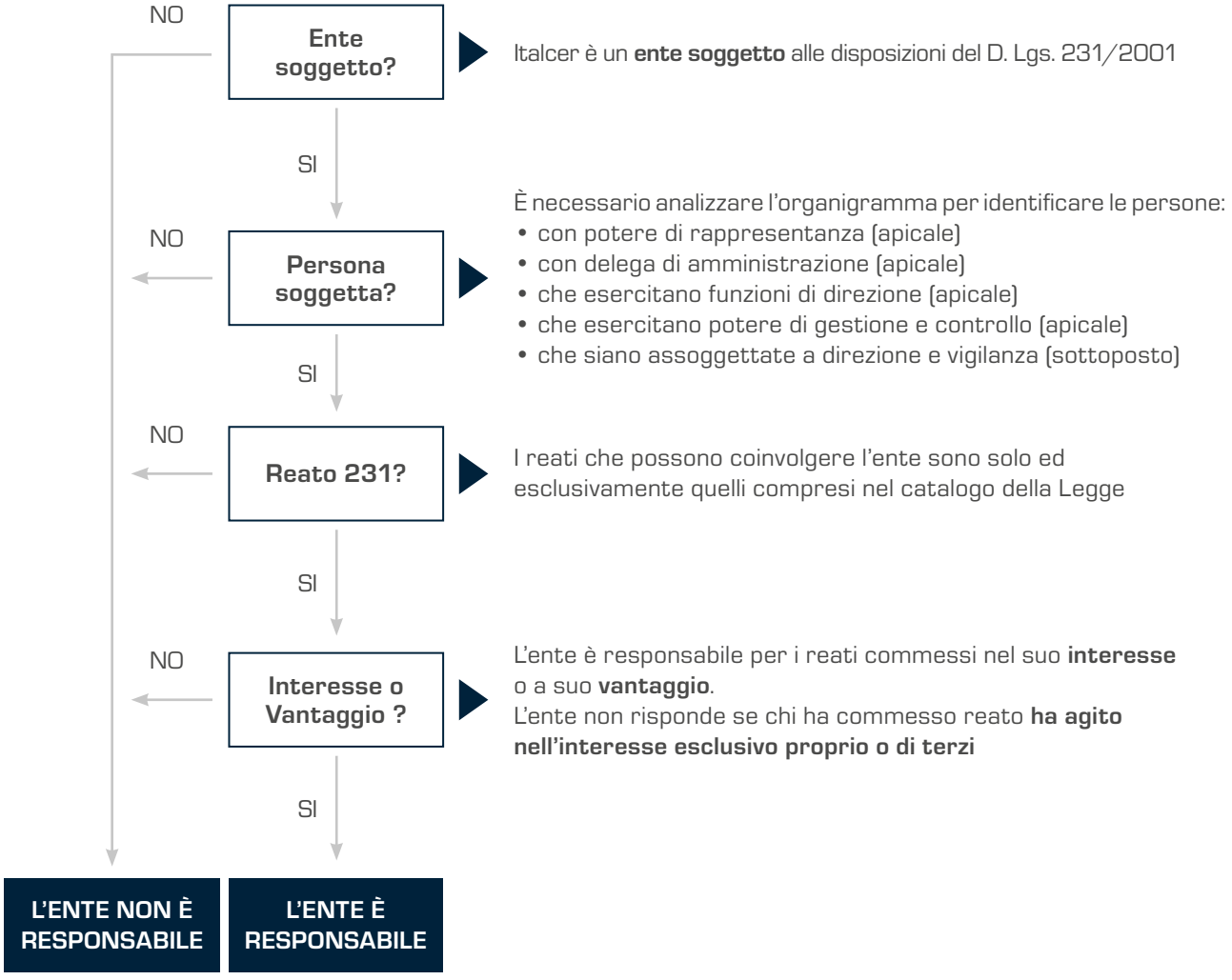
Il presente documento, pubblicato sul sito web della Società, ha lo specifico scopo di illustrare le linee guida che hanno ispirato l'adozione e l'attuazione del Modello stesso, attraverso l'approfondimento dei relativi passaggi applicativi.

L'Amministratore Delegato
Dott. Graziano Verdi

Indice

1
I meccanismi di funzionamento del D. Lgs. 231/2001

Il D. Lgs. 231/2001 estende agli enti le conseguenze delle condotte penalmente rilevanti intrattenute dalle persone fisiche che operano al suo interno come amministratori, dipendenti o consulenti. Il coinvolgimento dell'azienda si verifica al **combinarsi simultaneo** di 4 condizioni:



1.1 Il catalogo dei reati

Le sanzioni previste dal D. Lgs. 231/2001 si applicano ad una platea di reati molto ampia.

Di seguito sono state isolate le categorie di reato che, con diverso livello di rischio, possono costituire le aree sensibili di applicazione della legge per la nostra Società:

1. Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della **salute** e sicurezza sul lavoro
2. Reati **Ambientali**
3. Reati **Informatici**
4. Reati contro la **Pubblica Amministrazione**
5. Reati **Societari e Tributari**

1.2 Il coinvolgimento presunto dell'ente

Il D. Lgs. 231/2001 stabilisce una sorta di **automatismo**. Quando una figura apicale o sottoposta commette uno dei reati previsti dal decreto **nell'interesse** o **a vantaggio** dell'ente per cui lavora, L'ENTE È SEMPRE RESPONSABILE, a meno che lo stesso non abbia messo in atto le opportune contromisure di prevenzione e controllo.

QUALI?

- dimostrare di aver messo in atto le giuste contromisure atte a **prevenire e controllare** la condotta di chi ha commesso reato
- dimostrare che chi ha eventualmente commesso il reato, lo ha fatto **violando fraudolentemente** il sistema di prevenzione e controllo

Il sistema di contromisure e/o presidi si chiama **MODELLO ORGANIZZATIVO** (o modello organizzativo di gestione e controllo c.d. **MOGC**). Se un ente è in grado di dimostrare l'esistenza delle contromisure e/o dei presidi, vuol dire che è dotato di un MOGC, ossia dell'insieme di regole e procedure atte a prevenire e controllare la commissione dei reati previsti nel decreto da parte dei propi soggetti apicali o sottoposti. In caso di evento fatale (capo di imputazione per un apicale) l'esistenza del modello, prima ancora di mostrarsi nella sua efficienza, **PROTEGGE DALLE MISURE CAUTELARI CHE POTREBBERO SCATTARE A CARICO DELL'ENTE (ARTT. 49 e 17 del D.LGS. 231/2001)**.

1.3 La funzione di prevenzione e controllo del Modello Organizzativo

PREVENZIONE:

Formazione continua

Codice etico

Codice disciplinare

Policy e procedure

Organismo di Vigilanza (ODV)

ATTIVITÀ A BASSA COMPLESSITÀ

CONTROLLO:

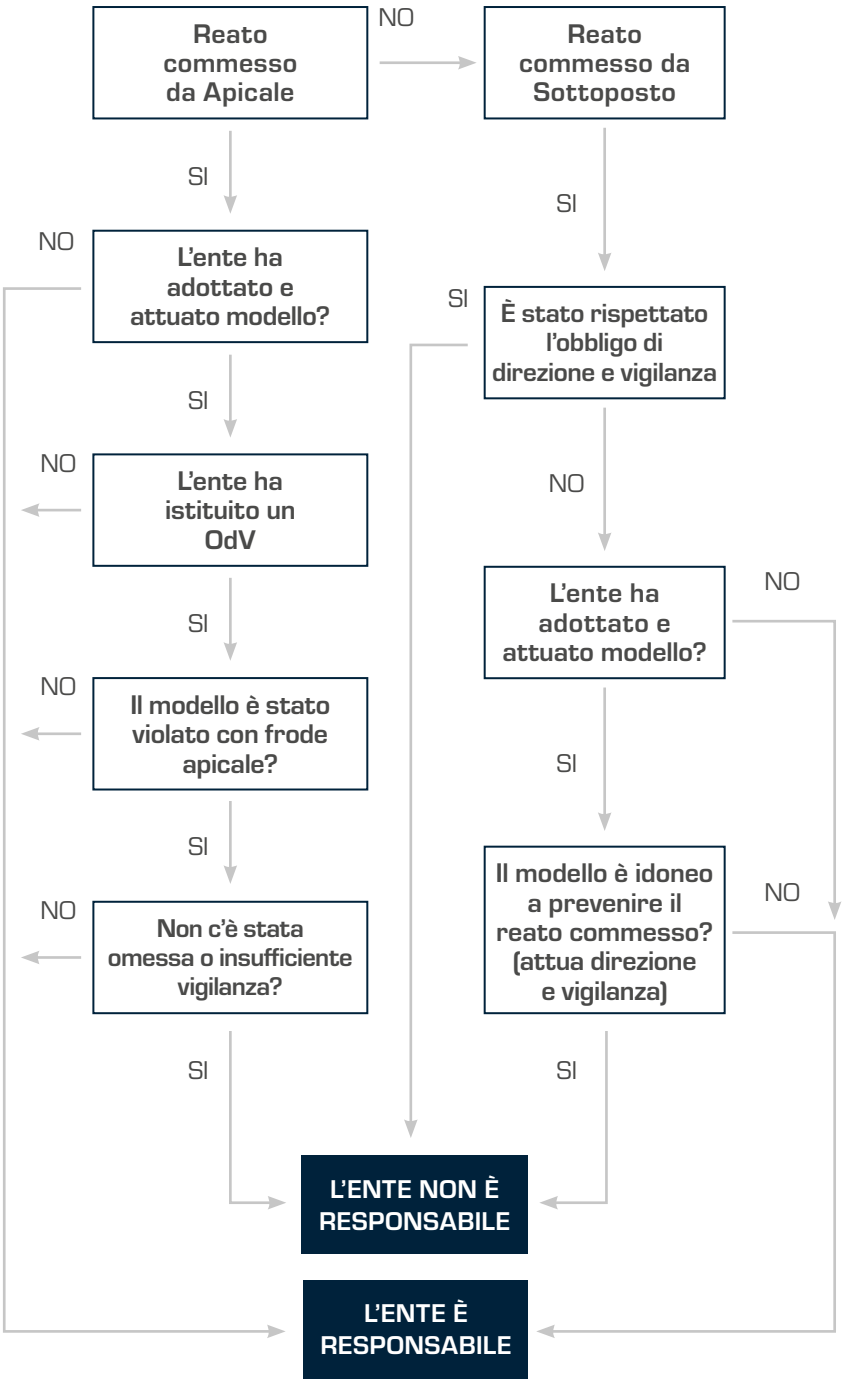
Flusso informativo periodico all'ODV e all'Internal Audit sullo stato di efficienza e di funzionamento del Modello Organizzativo

Flusso informativo all'ODV e all'Internal Audit sullo stato di aggiornamento legislativo e organizzativo del Modello Organizzativo

ATTIVITÀ AD ALTA COMPLESSITÀ

1.4 La funzione esimente del Modello Organizzativo

In caso di evento avverso, il Modello Organizzativo deve essere in grado di esercitare la funzione esimente innanzi all'autorità inquirente.



In caso di reato commesso da **Apicale** il MOGC è necessario perché l'ENTE per essere esentato **DEVE DIMOSTRARE** (inversione dell'onere della prova):

1. di aver messo in atto azioni di prevenzione quali:
   - aver **adottato** un MOGC
   - averlo **attuato**
   - avere **vigilato** sul suo funzionamento;
2. che la figura apicale che ha commesso il reato, lo abbia fatto **aggirando fraudolentemente** il MOGC;
3. che **l'ODV abbia vigilato** sul MOGC non attuando comportamenti omissivi o negligenti.

In caso di reato commesso da **sottoposto,** il MOGC è necessario perché l'ENTE per essere esentato DEVE evitare che il **PM DIMOSTRI che**:

1. la commissione del reato è stata resa possibile **dall'inosservanza** degli **obblighi** di **direzione** e **vigilanza** da parte degli apicali, oppure
2. esiste un modello organizzativo che prevede la direzione e la vigilanza da parte degli apicali sui sottoposti, che detto modello **non risponda** ai **criteri** di **efficienza** o che i meccanismi di direzione e vigilanza non abbiano funzionato.

2
Implementazione del MOGC

ANALISI PRELIMINARE DEL CONTESTO

- Analisi dell'attività esercitata
- Ciclo passivo
- Ciclo attivo
- Ciclo di produzione con descrizione fisica e giuridica del layout produttivo
- Analisi del contesto sociale e industriale in cui opera la società
- Informazioni sul personale dipendente
- Informazioni sull'infrastruttura tecnologica
- Informazioni sulla struttura dei controlli interni ed esterni.

RISK ASSESSMENT

- Identificazione delle potenziali aree di Rischio 231
- Valutazione del rischio inerente e del rischio residuo per ciascuna singola area
- Classificazione delle aree in funzione del grado di rischiosità
- Misurazione del GAP tra conformità attuale e compliance teorica del 100%

PIANO DI RIMEDIO

Deriva dal Risk Assessment e viene svolto annualmente evidenziando le azioni di rimedio in funzione dell'urgenza con cui devono essere messe in atto. Fornisce uno strumento di controllo sullo stato di avanzamento del lavoro di compliance.

CODICE ETICO

Italcer Group si è dotato di un Codice Etico che rappresenta lo strumento fondamentale per salvaguardare e tramandare i valori e i principi più autentici che rappresentano i veri pilastri della filosofia imprenditoriale del Gruppo. Nello specifico, il Codice Etico rappresenta l'insieme dei principi positivi e delle regole di comportamento che le società del Gruppo hanno scelto volontariamente di adottare e rendere pubblici, come concreta espressione dei lori propositi verso gli stakeholder.

CODICE DISCIPLINARE

Il Codice disciplinare, all'interno del Modello Organizzativo 231, riveste un ruolo di fondamentale importanza nel garantire il rispetto e la conformità al Modello Organizzativo stesso. Le sue finalità principali sono progettate per preservare l'integrità, la legalità e la corretta applicazione delle norme e delle regolamentazioni aziendali.

FORMAZIONE CONTINUA

La formazione continua viene messa in atto sin dal giorno dell'adozione del MOGC ed è prevalentemente svolta in aula con sistemi di valutazione dell'apprendimento.

Parte generale

Contiene i principi fondamentali del sistema di gestione del rischio, tra cui il quadro normativo di riferimento, gli obiettivi del MOGC, il codice etico, il sistema disciplinare e i compiti dell'Organismo di Vigilanza.

1. Company profile
2. Meccanismi di funzionamento del D.lgs. 231/2001
3. Le funzioni Audit, Risk e Compliance (ARC) per il MOGC
4. Attuazione del modello organizzativo 231
5. La digitalizzazione del modello organizzativo dinamico

Parte speciale

Entra nel dettaglio delle singole categorie di reato presupposto previste dal D.Lgs. 231/2001, identificando le aree a rischio e le misure di prevenzione specifiche adottate dalla Società per ciascuna tipologia di illecito.

Le sue componenti sono:

1. Informazioni aziendali propedeutiche all'adozione e implementazione del Modello Organizzativo ex D.Lgs. 231
2. Il Risk assessment
3. Gli strumenti di prevenzione in vigore (codice etico e codice disciplinare, piano di formazione)
4. Gli strumenti di segnalazione
5. Modalità di gestione dei dati sensibili
6. Piano di rimedio

La gestione del MOGC di Italcer si avvale di un repository di documenti e processi correlati atti a prevenire e controllare la commissione dei reati 231. Il repository si fonda su un organigramma interattivo e un sociogramma che permettono di collegare ogni singola risorsa umana ai processi che gestisce o in cui è coinvolta, tracciandone le storicità.

2.1 Il Risk Assessment

2.1.1 Definizioni

Il rischio inerente rappresenta il livello di esposizione di un'organizzazione a un determinato evento potenzialmente dannoso, calcolato prima dell'applicazione di qualsiasi misura di controllo o mitigazione. Si tratta di un rischio "puro" e intrinseco al processo, all'attività o all'ambiente operativo in cui l'organizzazione opera.

Il rischio residuo rappresenta invece il livello di rischio che "residua" dopo l'implementazione, anche parziale, di misure di controllo, mitigazione e prevenzione. Prima ancora di implementare dette misure, è il rischio che l'organizzazione continua a correre, nonostante l'esistenza di procedure e sistemi di gestione. In altri termini, in assenza di contromisure, il rischio residuo corrisponde al rischio inerente.

La probabilità rappresenta la frequenza stimata o la possibilità che un evento rischioso si verifichi in un determinato contesto e dipende da vari fattori intrinseci ed estrinseci all'attività o al processo analizzato.

L'impatto rappresenta invece la gravità delle conseguenze che un evento rischioso può causare. Riflette il livello di danno o perdita potenziale in termini economici, normativi, operativi, reputazionali o ambientali.

2.1.2 Metodologia

1. Identificazione delle potenziali **aree di rischio** applicabili all'ente
2. Valutazione del **rischio inerente** e del **rischio residuo** per ciascuna singola area
3. **Classificazione** delle aree in funzione del grado di rischiosità
4. Misurazione del **«GAP»** tra contesti con rischio residuo reale e contesti con rischio residuo teorico nullo
5. Individuazione delle **azioni di rimedio e/o di mitigazione dei rischi**
6. Definizione di un **remediation plan** per l'esecuzione delle azioni individuate

2.1.3 Impiego dell'intelligenza artificiale

L'impiego dell'IA consente di sintetizzare le prime 5 attività sopra menzionate in un unico processo attraverso algoritmi consequenziali, alla base dei seguenti passaggi:

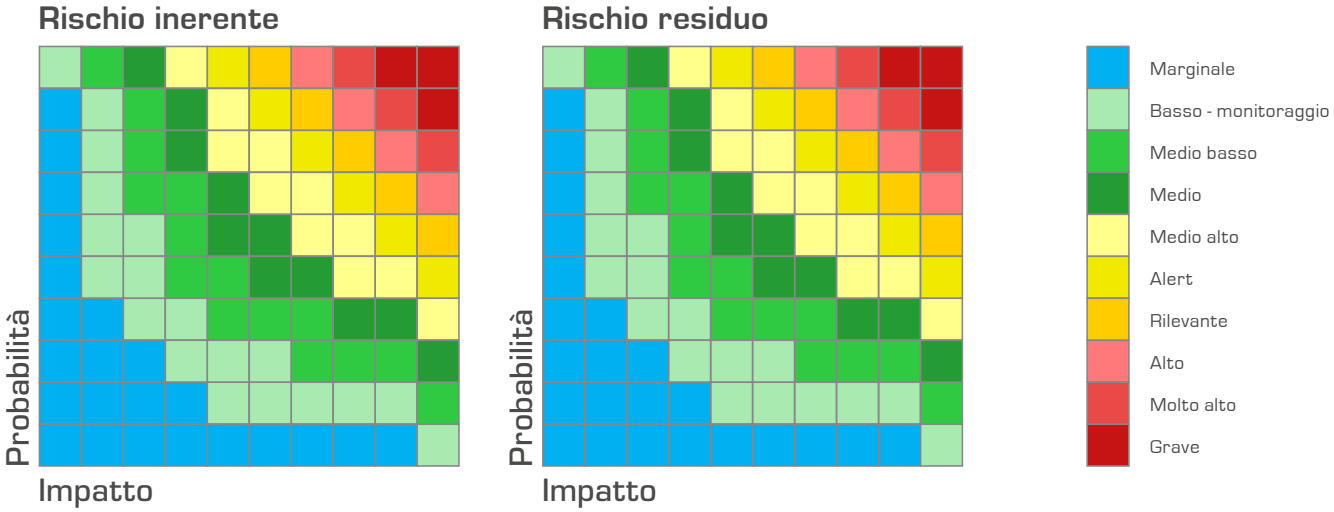
1. Creazione di check-list personalizzate
2. Compilazione delle check-list
3. Creazione dell'algoritmo per ottenere risposte per ogni categoria di reato in termini di valutazione del rischio inerente e rischio residuo sulla base delle probabilità di evenienza e dell'eventuale impatto
4. Generazione della valutazione dei rischi inerente e residuo
5. Generazione delle azioni di rimedio.

L'algoritmo elabora i dati su quattro livelli:

- **livello 1:** sulla fattispecie di reato e le sue condotte
- **livello 2:** su contesti della fattispecie di reato individuati dall'algoritmo (da 1 a N contesti)
- **livello 3:** per ogni contesto, misurazione di probabilità e impatto dell'evento con riferimento al rischio inerente (da 1 a 10 gradi)
- **livello 4:** per ogni contesto, misurazione di probabilità e impatto con riferimento al rischio residuo (da 1 a 10 gradi).

LIVELLO 1	LIVELLO 2	LIVELLO 3	LIVELLO 4
REATO	CONTESTO	RISCHIO INERENTE	RISCHIO RESIDUO
	Contesto 1	Probabilità (da 1a10)	Probabilità (da 1a10)
		Impatto (da 1 a 10)	Impatto (da 1 a 10)
	Contesto 2	Probabilità (da 1a10)	Probabilità (da 1a10)
		Impatto (da 1 a 10)	Impatto (da 1 a 10)
	Contesto N	Probabilità (da 1a10)	Probabilità (da 1a10)
		Impatto (da 1 a 10)	Impatto (da 1 a 10)

		RISCHIO INERENTE	RISCHIO RESIDUO
VALUTAZIONE FINALE	1	Marginale	Marginale
	2	Basso	Basso
	3	Medio basso	Medio basso
	4	Medio basso	Medio basso
	5	Medio alto	Medio alto
	6	Alert	Alert
	7	Rilevante	Rilevante
	8	Alto	Alto
	9	Molto alto	Molto alto
	10	Grave	Grave



2.1.4 Individuazione delle variabili di primo livello

	FATTISPECIE DI REATO	AREA DI RISCHIO - REATI	GRADO DI RILEVANZA AI FINI DEL RISK ASSESSMENT	AZIONI
1	INDEBITA PERCEZIONE DI EROGAZIONI, TRUFFA IN DANNO DELLO STATO, FRODE NELLE PUBBLICHE FORNITURE E FRODE INFORMATICA (ART. 24)	Contro lo stato - 24	Rischio potenziale – necessario risk assessment	Risk assessment
2	DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI (ART. 24-BIS)	Informatici - 24bis	Rischio potenziale – necessario risk assessment	Risk assessment
3	DELITTI DI CRIMINALITÀ ORGANIZZATA (ART. 24-TER)	Criminalità organizzata (24ter)	Condotta non applicabile con rischio reale nullo	Nessuna
4	PECULATO, CONCUSSIONE, INDUZIONE INDEBITA, CORRUZIONE E ABUSO D'UFFICIO (ART. 25)	Corruzione concussione - 25	Condotta applicabile ma con rischio inerente nullo	Monitoraggio
5	FALSITÀ IN MONETE, CARTE DI PUBBLICO CREDITO E VALORI DI BOLLO (ART. 25-BIS)	Falsità in monete - 25.2	Condotta non applicabile – non necessario risk assessment	Nessuna
6	DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO (ART. 25-BIS.1)	Delitti Industria e commercio (25.2.1)	Rischio residuo alto – necessario risk assessment	Monitoraggio
7	REATI SOCIETARI (ART. 25-TER)	Societari (25.3)	Rischio potenziale – necessario risk assessment	Risk assessment
8	REATI CON FINALITÀ DI TERRORISMO O EVERSIONE DELL'ORDINE DEMOCRATICO (ART. 25-QUATER)	Terrorismo e eversione (25.4)	Condotta non applicabile – non necessario risk assessment	Nessuna
9	PRATICHE DI MUTILAZIONE DEGLI ORGANI GENITALI FEMMINILI (ART. 25-QUATER.1)	Mutilazione (25.4.1)	Condotta non applicabile – non necessario risk assessment	Nessuna
10	DELITTI CONTRO LA PERSONALITÀ INDIVIDUALE (ART. 25-QUINQUIES)	Personalità individuale (25.5)	Condotta non applicabile – non necessario risk assessment	Nessuna
11	REATI DI ABUSO DI MERCATO (ART. 25-SEXIES)	Abuso di mercato (25.6)	Condotta non applicabile – non necessario risk assessment	Nessuna
12	OMICIDIO COLPOSO E LESIONI PERSONALI COLPOSE IN VIOLAZIONE DELLE NORME SULLA SICUREZZA SUL LAVORO (ART. 25-SEPTIES)	Sicurezza sul lavoro (25.7)	Rischio inerente sensibile – necessario risk assessment	Risk assessment
13	RICETTAZIONE, RICICLAGGIO, IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA E AUTORICICLAGGIO (ART. 25-OCTIES)	Riciclaggio e auto riciclaggio (25.8)	Rischio inerente nullo anche se potenziale - necessario monitoraggio	Monitoraggio

	FATTISPECIE DI REATO	AREA DI RISCHIO - REATI	GRADO DI RILEVANZA AI FINI DEL RISK ASSESSMENT	AZIONI
14	STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI (ART. 25-OCTIES.1)	Strumenti di pagamento (25.8.1)	Condotta non applicabile – non necessario risk assessment	Nessuna
15	VIOLAZIONE DEL DIRITTO D'AUTORE (ART. 25-NOVIES)	Diritto d'autore (25.9)	Rischio inerente nullo anche se potenziale - necessario monitoraggio	Monitoraggio
16	INDUZIONE A NON RENDERE DICHIARAZIONI ALL'AUTORITÀ GIUDIZIARIA (ART. 25-DECIES)	False dichiarazioni (25.10)	Condotta applicabile ma con rischio nullo	Nessuna
17	REATI AMBIENTALI (ART. 25-UNDECIES)	Sicurezza ambientale (25.11)	Rischio inerente elevato – necessario risk assessment	Risk assessment
18	IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE (ART. 25-DUODECIES)	Impiego irregolare MOD (25.12)	Rischio potenziale ma nullo nella pratica - non necessario risk assessment	Nessuna
19	RAZZISMO E XENOFOBIA (ART. 25-TERDECIES)	Razzismo (25.13)	Rischio potenziale ma nullo nella pratica - non necessario risk assessment	Nessuna
20	FRODE IN COMPETIZIONI SPORTIVE (ART. 25-QUATERDECIES)	Frode sportiva (25.14)	Condotta non applicabile – non necessario risk assessment	Nessuna
21	REATI TRIBUTARI (ART. 25-QUINQUIESDECIES)	Reati tributari (25.15)	Rischio potenziale – necessario risk assessment	Risk assessment
22	CONTRABBANDO (ART. 25-SEXIESDECIES)	Contrabbando (25.16)	Condotta non applicabile – non necessario risk assessment	Nessuna
23	REATI TRANSNAZIONALI (ART. 10 DELLA L. 146/2006)	Transnazionali	Condotta applicabile ma con rischio nullo	Nessuna
24	SICUREZZA INFORMATICA DELLE INFRASTRUTTURE CRITICHE	Sicurezza informatica	Compresa nel risk assessment dei reati informatici	Inclusa nel risk assessment

2.1.5 Individuazione delle variabili di secondo livello - aree maggior rischio

AREA SICUREZZA SUL LAVORO

- Utilizzo di check-list basate sulle prescrizioni del D. Lgs. 81 del 2008
- Mappatura delle prescrizioni e linee guida INAIL
- Integrazione con certificazioni ISO ottenute (ISO 9001, ISO 14001, ISO 450001, ISO 50001)

AREA SICUREZZA AMBIENTALE

- Utilizzo di check-list basate su dati aziendali come (i) numero impianti, (ii) dimensione media impianti, (iii) grado di automazione della produzione, (iv) turni di produzione, (v) età media degli impianti, (vi) personale coinvolto, ecc.
- Valutazione per ogni impianto della rischiosità in base alla classificazione dell'ARPA nazionale in relazione a (i) inquinamento del suolo, (ii) inquinamento del sottosuolo, (iii) inquinamento idrico, (iv) inquinamento dell'aria e (v) smaltimento rifiuti

AREA SICUREZZA INFORMATICA

- Valutazione del verificarsi delle minacce di incident previste dall'autorità europea per il controllo della pirateria informatica (ENISA) ovvero: (i) ransomware, (ii) malware, (iii) cryptojacking, (iv) attacchi alla posta elettronica (e-mail), (v) attacchi ai dati, (vi) Attacchi web, (vii) disinformazione e (viii) misinformazione.

AREA REATI SOCIETARI

- Valutazione sulla base di check-list che tengono conto di (i) contesto aziendale; (ii) sistemi di controllo interni (quali procedure e protocolli dell'internal audit, del C.F.O. e della funzione IT) ed esterni (società di revisione, collegio sindacale e Organismo di Vigilanza).

AREA REATI TRIBUTARI

- Valutazione sulla base di check-list che tengono conto di: (i) contesto aziendale; (ii) interazione con soggetti esteri (principalmente clienti) situati in tutti i territori del mondo; (ii) criticità delle transazioni internazionali; (iv) procedure di selezione fornitori e KYC sulla clientela.

AREA REATI CONTRO LO STATO

- Valutazione sulla base di check-list redatte prendendo a riferimento le linee guida dell'ENAC (Ente Nazionale Anti Corruzione), e tenendo conto di (i) contesto aziendale; (ii) ciclo attivo e passivo e assenza di interazione con enti pubblici; (iii) percezione di finanziamenti e contributi pubblici.

2.2 il Piano di rimedio - un estratto

TASK PIANO DI RIMEDIO		MESI 2025								
Sicurezza sul lavoro (art. 25 - septies)	**Responsabile task**	4	5	6	7	8	9	10	11	12
Azione di mitigazione/rimedio										
Azione di mitigazione/rimedio										
Reati ambientali (art. 25 - undecies)	**Responsabile task**									
Azione di mitigazione/rimedio										
Azione di mitigazione/rimedio										
Reati informatici (art. 24 - bis)	**Responsabile task**									
Azione di mitigazione/rimedio										
Azione di mitigazione/rimedio										
Reati contro lo Stato (art. 24)	**Responsabile task**									
Azione di mitigazione/rimedio										
Azione di mitigazione/rimedio										
Reati societari (art. 25 - ter)	**Responsabile task**									
Azione di mitigazione/rimedio										
Azione di mitigazione/rimedio										

L'Internal Audit e l'Organismo di Vigilanza controllano l'esecuzione del piano di rimedio sulla base di un piano di audit che viene condiviso dal Consiglio di Amministrazione.

Il sistema fornisce report appropriati sia per l'Organismo di vigilanza che per l'Internal Audit.

3
Manutenzione e aggiornamento periodico del MOGC

NUOVO RISK ASSESSMENT

Revisione dei risk assessment su tre direttrici:

1. Analisi dello **stato di avanzamento delle attività** di cui al piano di rimedio dell'anno precedente
2. **Variazioni nelle informazioni di contesto** (ciclo attivo, passivo, ciclo di produzione, diversificazioni, differenziazione, apertura nuovi mercati, ecc.)
3. **Variazioni normative oggettive** delle leggi che regolamentano la compliance delle aree di rischio

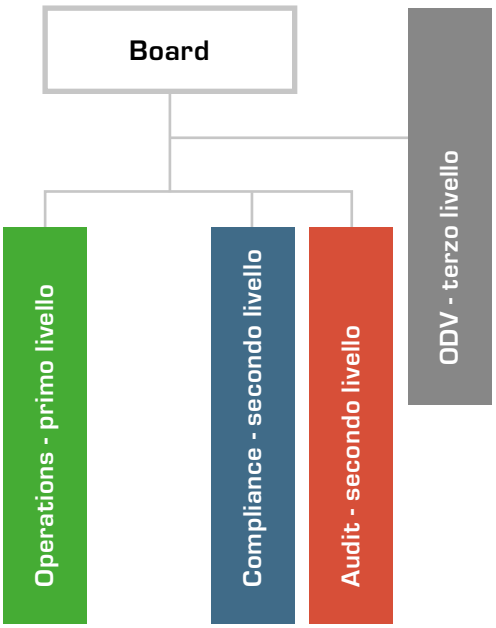
NUOVO PIANO DI RIMEDIO

Revisione delle **azioni di rimedio** da implementare in conseguenza delle modifiche al Risk assesment.

NUOVO PIANO DI AUDIT

A fronte del piano di rimedio viene emesso il nuovo **piano di audit.**

4
La funzione di controllo



La funzione di controllo di Italcer è impostata su tre livelli:

controllo di primo livello sulle *operation*, sulla base delle singole procedure operative, eseguito dai responsabili di funzione ai vari livelli dell'organigramma;

controllo di secondo livello eseguito dalla funzione Compliance & internal Audit, individuata in una figura manageriale, anche membro interno dell'Organismo di Vigilanza, con accesso al repository;

controllo di terzo livello eseguito dall'Organismo di Vigilanza nominato dal Consiglio di Amministrazione e dotato di autonomia di spesa;

L'Internal Audit può essere contattato al seguente indirizzo email:
audit@gruppoitalcer.it

5
L'Organismo di Vigilanza

Ai sensi degli articoli 6, 7 e 8 del D. Lgs. 231 del 2001, il Consiglio di Amministrazione che ha approvato il Modello Organizzativo ha anche nominato un Organismo di Vigilanza collegiale, composto da 3 membri che si sono dotati di un autonomo regolamento, oltre ad essere stato dotato di budget autonomo di spesa.

L'Organismo di Vigilanza in carica è composto dai seguenti membri:

- Dott. Giovanni Taliento
- Dott.ssa Ilaria Patri
- Avv. Marika Rossi

L'Organismo di Vigilanza può essere contatto al seguente indirizzo email:
organismodivigilanza@gruppoitalcer.it

6
Il Whistleblowing

Con la Legge 30 novembre 2017, n. 179 recante le "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato" (nel seguito, anche, "Legge sul Whistleblowing") il Legislatore, nel tentativo di armonizzare le disposizioni previste per il settore pubblico con la richiamata Legge, ha introdotto specifiche previsioni per gli enti destinatari del D. Lgs. n. 231/2001 ed ha inserito all'interno dell'art. 6 del D. Lgs. n. 231/2001 tre nuovi commi, ossia il comma 2-bis, 2- ter e 2-quater.

Il nostro Modello Organizzativo prevede che i Destinatari, che nello svolgimento dei propri compiti, rilevino o vengano a conoscenza di possibili comportamenti illeciti o irregolarità posti in essere da soggetti che hanno a vario titolo rapporti con la Società, siano tenuti a segnalare senza indugio i fatti, gli eventi e le circostanze che gli stessi ritengano, in buona fede e sulla base di ragionevoli elementi di fatto, aver determinato tali violazioni e/o condotte non conformi ai principi della Società.

Le segnalazioni dovranno essere trasmesse per mezzo di un canale riservato e gestito, accessibile al seguente link: **https://italcer.integrityline.com**

ITALCER GROUP

DESIGN SURFACES

WWW.GRUPPOITALCER.IT