ITALCER

MODELLO ORGANIZZATIVO
EX D. LGS. 231/2001

Linee guida per l'implementazione ed il funzionamento

ELIOS ceramica

CERAMICA Rondine italiani per stile

BOTTEGA

Premessa

Il 14 dicembre 2021 il Consiglio di Amministrazione ha approvato l'adozione del Modello di Organizzazione, Gestione e Controllo (di seguito anche «Modello») ai sensi del D. Lgs. 231/2001.

Inoltre, nella stessa sede, veniva nominato l'Organismo di Vigilanza (di seguito anche «OdV») in composizione collegiale, il quale ha provveduto a consegnare il proprio Regolamento nonché il piano di audit.

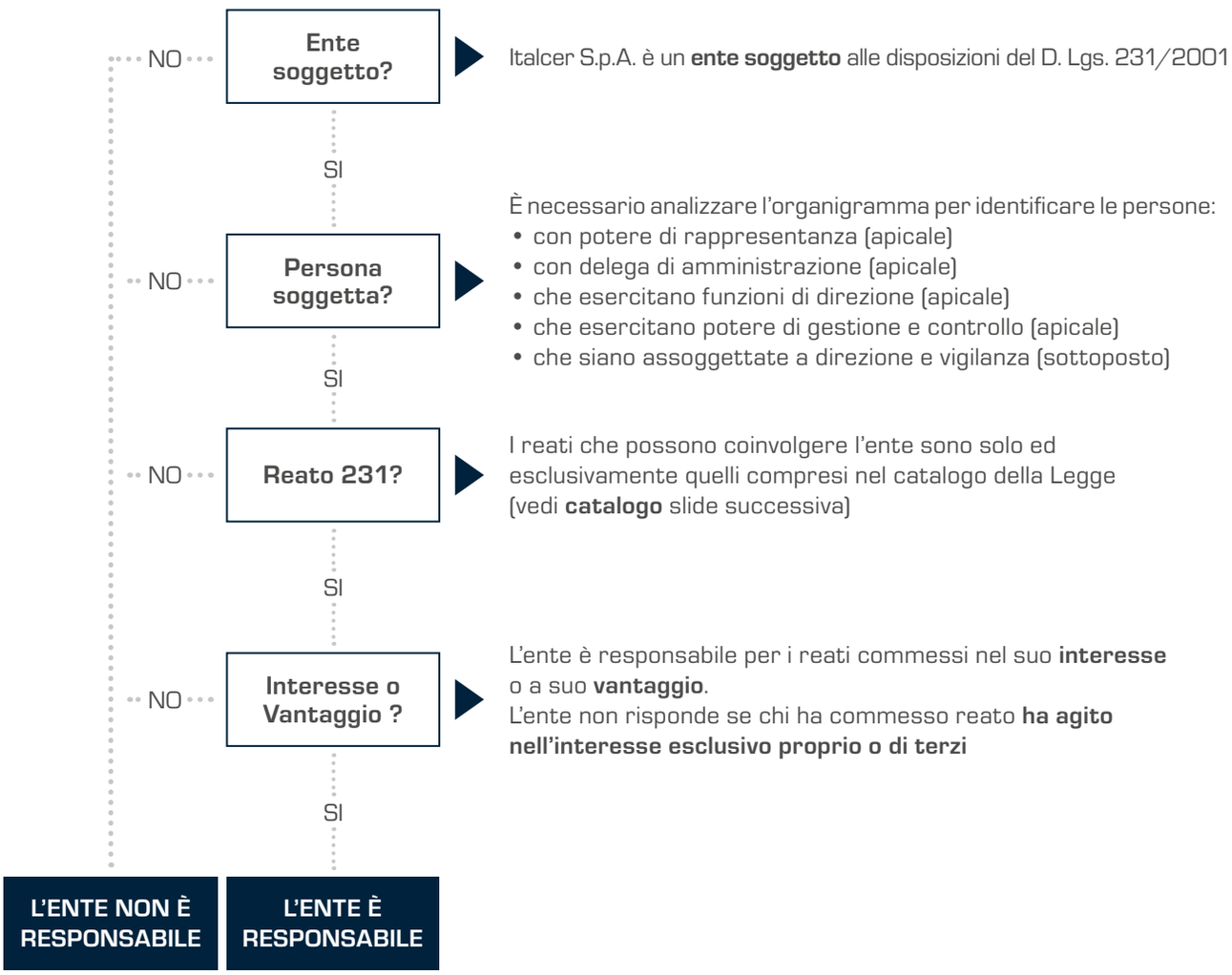
Il presente documento, pubblicato sul sito web della società, ha il precipuo scopo di illustrare le linee guida che hanno ispirato l'attuazione e l'adozione del Modello stesso, attraverso l'approfondimento dei relativi passaggi applicativi.

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 (1/2)

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

1. Indebita percezione di erogazioni, **truffa in danno dello Stato** o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico
2. **Delitti informatici** e illecito trattamento di dati
3. Delitti di **criminalità organizzata**, anche transnazionale
4. **Concussione**, induzione indebita a dare o promettere utilità e **corruzione**
5. **Falsità in monete**, in carte di pubblico credito e in valori di bollo in strumenti o **segni di riconoscimento**
6. **Delitti in materia di strumenti di pagamento diversi dai contanti**
7. Reati **contro l'industria** e il **commercio**
8. Reati **societari**
9. Delitti con finalità di **terrorismo** o di **eversione** dell'ordinamento democratico
10. Pratiche di **mutilazione** degli organi genitali femminili
11. Delitti contro la **personalità individuale**
12. **Abusi** di mercato
13. Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della **salute** e **sicurezza** sul **lavoro**
14. **Ricettazione**, **riciclaggio** e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio
15. Delitti in materia di violazione del **diritto d'autore**
16. Induzione a **non rendere** dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria
17. Reati **ambientali**
18. **Impiego** di **cittadini** di Paesi terzi il cui soggiorno è **irregolare**
19. Reati di **razzismo** e **xenofobia**
20. Reati di **frode sportiva**
21. Reati **tributari**
22. **Reati transazionali**
23. **Contrabbando**
24. Reati contro il patrimonio culturale

1.1 Il catalogo dei reati (2/2)

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. Indebita percezione di erogazioni, **truffa in danno dello Stato** o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico
2. **Delitti informatici** e illecito trattamento di dati
3. **Concussione**, induzione indebita a dare o promettere utilità e **corruzione**
4. Reati **societari**
5. Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della **salute** e **sicurezza** sul **lavoro**
6. **Ricettazione**, **riciclaggio** e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio
7. Reati **ambientali**
8. Reati **tributari**.

Per una analisi più approfondita della Legge e delle categorie di reato descritte negli articoli dal 24 al 26, nonché per un pronto collegamento ipertestuale agli articoli del codice penale richiamati, si rimanda al seguente link disponibile presso il sito web ufficiale dello Stato: DECRETO 31 maggio 2001, n. 321 - Normattiva

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 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. **MOCG**). Se un ente è in grado di dimostrare l'esistenza delle contromisure e/o dei presidi, vuol dire che è dotato di un MOGC 231, ovvero dell'insieme di regole e procedure atte a prevenire e controllare la commissione dei reati previsti nel decreto da parte dei suoi apicali (ovvero 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)**.

La legge è molto **PRECISA** nell'indicare le prescrizioni che deve avere adottato l'ente che non vuole essere trascinato dalle condotte illecite dei suoi *apicali*.

1.3 La funzione di prevenzione e controllo del modello

PREVENZIONE:

Policy e procedure

Formazione continua

Codice etico

Codice disciplinare

Organismo di Vigilanza (ODV)

ATTIVITÀ A BASSA COMPLESSITÀ

CONTROLLO:

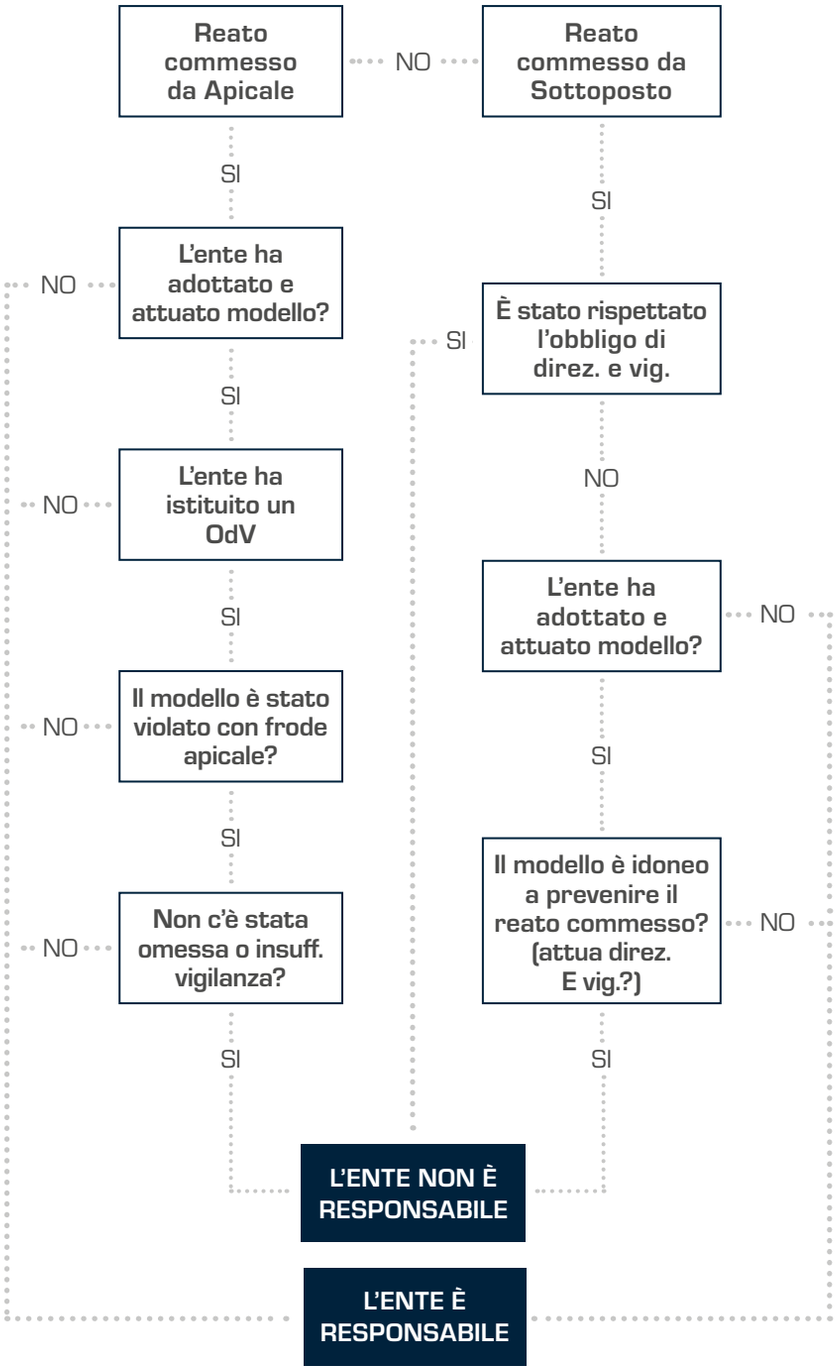
Flusso informativo periodico all'ODV sullo stato di efficienza e di funzionamento del modello organizzativo

Flusso informativo all'ODV sullo stato di aggiornamento legislativo e organizzativo del modello

ATTIVITÀ AD ALTA COMPLESSITÀ

1.4 La funzione esimente del modello

In caso di evento avverso, il Modello deve essere in grado di esercitare la funzione esimente nei confronti dell'autorità inquirente.



In caso di reato commesso da **Apicale** il MOCG 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 MOCG
   - averlo **attuato**
   - avere **vigilato** sul suo funzionamento;
2. che la figura apicale che ha commesso il reato, lo abbia fatto **aggirando fraudolentemente** il MOCG
3. che **l'ODV abbia vigilato** sul MOGC non attuando comportamenti omissivi o negligenti.

In caso di reato commesso da **sottoposto** il MO 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
La metodologia

La progettazione ed implementazione del nostro Modello organizzativo si è sviluppata attraverso tre attività ben distinte ma connesse:

RISK ASSESSMENT

Il **Risk Assessment**, che ha l'obiettivo di conoscere e fotografare l'azienda, evidenziando, con una appropriata analisi il piano di azione per l'intervento, ovvero il piano operativo di audit 231

- **1. INQUADRAMENTO GENERALE**
- **2. ASSESSMENT SUL PERSONALE**
- **3. ASSESSMENT SUI REATI**
- **4. ACTION PLAN**

PROGETTAZIONE E IMPLEMENTAZIONE

La **Progettazione** e **Implementazione** vera e propria del Modello Organizzativo 231. Ovvero la predisposizione dei presidi di prevenzione e di controllo sulla base della valutazione del rischio inerente di ciascuna area

- **1. SETUP ORGANIZZATIVO**
- **2. SETUP DEI PRESIDI DI CONTROLLO**
- **3. SETUP DEGLI STRUMENTI DI PREVENZIONE**
- **MOG 231: stampa di tutta la procedura**

MONITORAGGIO

Infine, il **Monitoraggio** del Modello Organizzativo attraverso la verifica della sua costante adeguatezza nonché dei flussi informativi provenienti dai presidi di controllo e diretti all'ODV

- **1. MONITORAGGIO AGGIORNAMENTO DEL MODELLO**
- **2. MONITORAGGIO DEI FLUSSI INFORMATIVI**

3
Il risk assessment

Il **Risk Assessment** ha l'obiettivo di conoscere e fotografare l'azienda, evidenziando, con una appropriata analisi, il piano di azione per la progettazione ed implementazione del Modello organizzativo.

Il Risk Assessment è un'attività che viene svolta sia in fase progettuale che in fase di check-up periodico del Modello con il doppio obiettivo:

- di individuare nuove aree di intervento;
- verificare le azioni di remediation programmate in precedenti risk assessment.

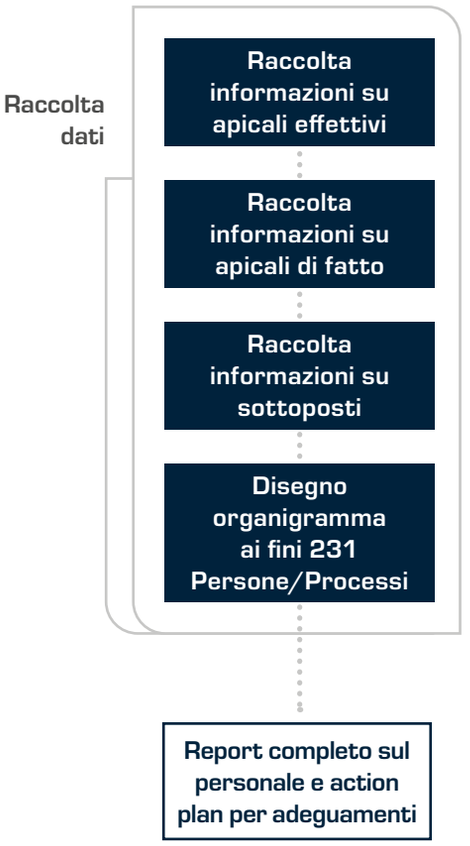
Il processo di Risk Assessment si compone delle attività di cui al flow riportato ed è caratterizzato da copiosa documentazione che è conservata agli atti della società, ma che è sempre consultabile online dai gestori del modello nonché da eventuali verificatori dello stesso.

3.1 Inquadramento generale della società

Inquadramento generale dell'azienda:
ha l'obiettivo di raccogliere informazioni per arrivare al disegno del ciclo attivo e del ciclo passivo aziendale, oltre che alle informazioni interne ed esterne di contesto, per addivenire gradualmente alla definizione delle macroaree a rischio di commissione dei reati di cui al catalogo del D. Lgs. 231/2001.

Modalità operativa di funzionamento e collegamenti:
l'attività è stata svolta con raccolta di documenti ed interviste ai diretti interessati. Le informazioni raccolte sono state catalogate in file che a loro volta contengono collegamenti ai documenti di supporto.

3.2 Il personale

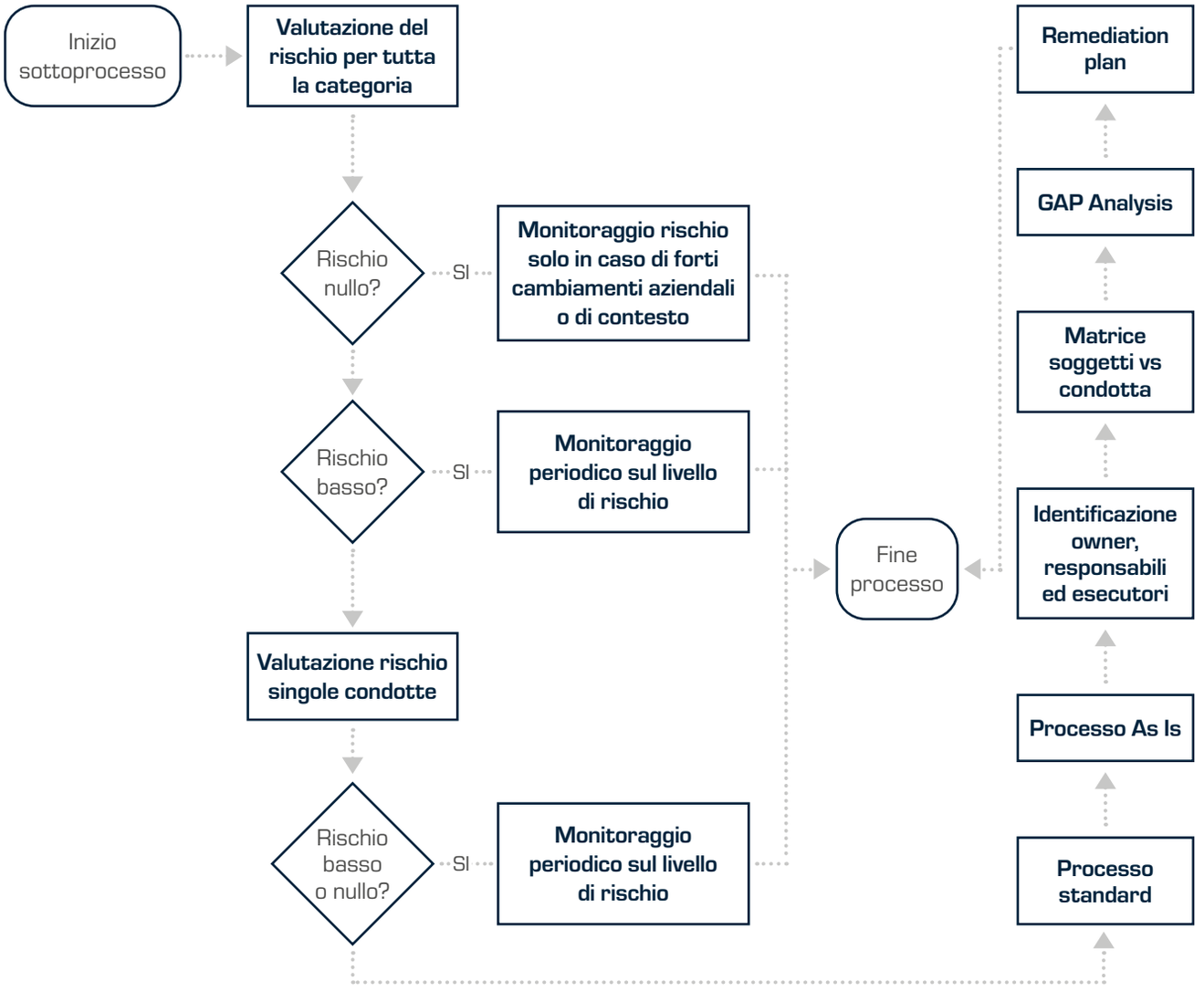


Assessment sul personale:
ovvero l'individuazione dei soggetti apicali e sottoposti, con raccolta di informazioni e documenti (deleghe, procure, job description, regolamenti interni) che il Modello tiene costantemente monitorati e aggiornati. L'obiettivo è il disegno dell'organigramma corrente e di quello «ideale 231», che correli i soggetti a rischio con i processi aziendali nei quali operano e con le potenziali condotte penalmente rilevanti che questi potrebbero intrattenere. Questa seconda fase (sovrapposizione con i reati) può essere completata solo dopo aver svolto l'assessment sulle condotte che mappano le aree sensibili.

Modalità operativa di funzionamento e collegamenti:
l'attività è stata svolta con la tracciatura di un primo organigramma corrispondente a quello in uso al momento di conduzione del primo risk assessment e che è stato utilizzato per evidenziare la gap analysis nei confronti di un organigramma ideale ai fini 231 che propone, in relazione ai dati anagrafici di ogni dipendente, le seguenti informazioni:

- Lettera di assunzione
- Job descritpion
- Deleghe
- Procure
- Processi sensibili di appartenenza
- Categoria di reati a rischio di condotta specifica nello svolgimento della propria mansione
- Status sulla formazione continua 231
- Classificazione in apicale o sottoposto ai fini della responsabilità diretta.

3.3 I reati



Assessment sui reati:
partendo da ciascun singolo reato e con riferimento alle condotte specifiche, l'attività ha l'obiettivo di valutare il «rischio inerente» del compimento di attività criminose da parte degli apicali individuati e collocati nei relativi processi di operatività. Particolare riguardo viene riservato ai presidi di controllo, sia facoltativi che obbligatori per legge, che vengono analizzati (con GAP Analysis mirata) mediante un approccio multidisciplinare in funzione della tipologia di attività esercitata dall'Ente.

Modalità operativa di funzionamento nella consultazione:
le carte di lavoro relative alle interviste ed alla raccolta delle informazioni in sede di primo risk assessment sono dinamicamente collegate alle aree di interesse:

- Area sicurezza sul lavoro
- Area sicurezza ambiente
- Area reati contro la PA
- Area reati societari
- Area reati tributari
- Area reati riciclaggio e autoriciclaggio
- Area reati informatici.

3.4 Descrizione delle attività del processo

- Valutazione del **rischio** in base alle informazioni di contesto: si tratta di una prima valutazione per categoria di reati che ha la precipua funzione di identificare quelli che hanno nulla o scarsa rilevanza nel contesto di riferimento.

- **Il processo standard**: ogni condotta è inquadrabile in un processo standard generalizzo che ha più la funzione di ausilio nell'indagine che di processo di riferimento senza escludere che possa esserlo. In altri termini, ha la funzione primaria di guidare l'analista e, opportunamente adattato, anche di rappresentare il presidio di controllo per l'azienda.

- Descrizione del **processo di presidio «As Is»**: attività volta a descrivere il processo che l'azienda attua per prevenire e controllare la condotta in esame. Questo processo costituisce il presidio di controllo sulla condotta che l'ente presenta al momento dell'indagine.

- Identificazione **dell'owner** di processo: ovvero individuazione dell'apicale (o degli apicali) referente di funzione.

- Identificazione del **responsabile**: ovvero identificazione di chi esercita il controllo delle operations. In funzione della dimensione delle azienda, owner e responsabile possono anche coincidere.

- Identificazione degli **esecutori**: ovvero individuazione del responsabile delle operations, colui che, opportunamente inquadrato in un processo, può costituire la funzione di audit di primo livello. L'esecutore può cioè controllare la conformità dell'atto che compie.

- **Sovrapposizione matriciale condotte/soggetti**: ovvero individuazione di una relazione biunivoca tra reato potenziale ed autore potenziale.

- **Gap Analysis**: ovvero determinazione dei «vuoti» di presidio/procedura rispetto ad una funzione reputata ideale ai fini 231.

- Eventuale **remediation plan**: ovvero definizione di un piano per il set-up del presidio ai fini 231 con la generazione dei flussi informativi a favore della funzione interna di audit e dell'Organismo di Vigilanza.

3.5 La metodologia di valutazione del rischio inerente (1/3)

Il rischio della commissione del reato (anche colposo) da parte di un apicale o da parte di un sottoposto, non soggetto ad adeguato controllo e coordinamento, è valutabile in base al combinarsi di due parametri di misurazione dell'evento avverso:

- La **probabilità** che l'evento si verifichi (**P**)
- Il **danno** che l'evento procura all'ente (**D**)

Il reato con rischio più alto è quello che combina un'alta probabilità con un danno elevato.
L'indice di probabilità (**P**) e l'indice di danno (**D**) possono essere misurati su diverse scale di valore.
Una scala troppo sintetica rischia di non riflettere la variabilità del dato.
Una scala troppo dettagliata rischia di mettere in crisi il grado di affinamento della valutazione da parte dell'analista sulle classi contigue.

3.5 La metodologia di valutazione del rischio inerente (2/3)

VALORE DI (P)	LIVELLO	DEFINIZIONE
4	**PIÙ CHE PROBABILE**	esiste una correlazione diretta tra il processo esaminato e la probabilità che la condotta possa essere intrattenuta. Sono fattori aggravanti il fatto che l'evento si sia già verificato o che la condotta venga reputata probabile dalle figure apicali stesse.
3	**MEDIAMENTE PROBABILE**	l'evento può verificarsi, anche non in maniera automatica o diretta. Sono elementi di valutazione in tal senso il numero di eventi passati o il grado di valutazione da parte degli owner di processo.
2	**SCARSAMENTE PROBABILE**	l'evento può prodursi solo in presenza di circostanze congiunturali.
1	**IMPROBABILE**	l'evento può verificarsi unicamente per la concomitanza di più concause indipendenti e poco probabili.

VALORE DI (D)	LIVELLO	DEFINIZIONE
4	**ALTO**	l'evento causa danni patrimoniali e non patrimoniali tali da incidere in maniera grave sul risultato dell'esercizio. Prevedibile un impegno finanziario rilevante ed un grave danno reputazionale.
3	**MEDIO**	l'evento produce danni patrimoniali e non patrimoniali tali da incidere in maniera negativa sul risultato dell'esercizio; Il danno reputazionale è riparabile.
2	**LIEVE**	l'evento genera un danno patrimoniale o non patrimoniale tale da non compromettere il risultato d'esercizio dell'ente.
1	**NULLO**	il verificarsi dell'evento non produce alcun danno all'ente.

3.5 La metodologia di valutazione del rischio inerente (3/3)

Il quadro di sintesi:

VALUTAZIONE RISCHIO COMMISSIONE REATO			DANNO			
			Basso	Lieve	Medio	Alto
			1	2	3	4
PROBABILITÀ	Improbabile	1	1	2	3	4
	Scarsamente probabile	2	2	4	6	8
	Mediamente probabile	3	3	6	9	12
	Più che probabile	4	4	8	12	16

- Rischio basso PxD <4
- Rischio lieve PxD <8
- Rischio medio PxD <12
- Rischio alto PxD >11

4
Organigramma

A seguito dell'attività di risk assessment è stato creato un organigramma funzionale al modello organizzativo che raccoglie le seguenti informazioni, già evidenziate in sede di raccolta dei dati relativi ai dipendenti:

- Lettera di assunzione
- Job descritpion
- Deleghe
- Procure
- Processi sensibili di appartenenza
- Categoria di reati a rischio di condotta specifica nello svolgimento della mansione
- Status sulla formazione continua 231
- Classificazione in apicale o sottoposto ai fini della responsabilità diretta.

5
Le aree di rischio ed i relativi presidi di controllo

Le aree di rischio individuate in funzione delle tipologie di condotta e del grado di rischio inerenti, sono le seguenti:

N.	Art	Tipologia	Condotta/Area sensibile
1	24	Reati contro la PA (Truffa/Malversazione)	Utilizzo fondi e contributi pubblici
			Richiesta fondi e contributi pubblici
2	24bis	Reati Informatici	Violazione dei dati aziendali
7	25ter	Reati Societari	False comunicazioni sociali
			Falso dei responsabili della rivisione
			Impedito controllo
			Formazione fittizia del capitale
12	25septies	Reati in tema di sicurezza sul lavoro	Lesioni colpose sui luoghi di lavoro
13	25octies	Reati riciclaggio e autoriciclaggio	Cessioni di beni core business
			Altre operazioni non ripetitive
			Finanziamenti di terzi
16	25undecies	Reati ambientali	Inquinamento rifiuti, emissioni
20	25quinquiesdecies	Reati tributari	Utilizzo di false fatture e altri artifizi
			Emissioni di fatture per operazioni inesistenti

6
Modalità di fornitura dei flussi informativi verso OdV e istruzioni operative per controllo e monitoraggio del Modello stesso

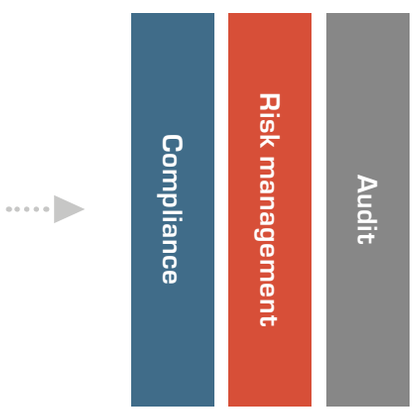
Il flusso informativo verso l'organismo di vigilanza avviene attraverso due principali modalità:
- Monitoraggio dei presidi di controllo
- Monitoraggio dell'adeguatezza del modello.

Monitoraggio dei presidi
All'interno di ogni sottoprocesso contenuto nei presidi di controllo delle aree di rischio è previsto un flusso informativo che prevede la segnalazione all'OdV di eventuali anomalie sui processi. Il controllo deve essere ovviamente attivato periodicamente dal responsabile di processo seguendo le indicazioni in esso riportate. È possibile che si debba procedere alla compilazione di specifiche check-list al fine di lasciare traccia del controllo effettuato. In caso di anomalie, il report all'ODV può contenere anche il piano di remediation (o piano di audit 231) che costituirà a sua volta elemento da tenere sotto osservazione per il successivo controllo.
In funzione del grado di rischio o della complessità del processo, il controllo può essere trimestrale o semestrale.
Infine, in funzione di alert estemporanei, è possibile procedere a verifiche non programmate e/o pianificate.

Monitoraggio del modello
Sempre con cadenza semestrale, devono essere assoggettate a specifici assessment le variabili che determinano un'azione integrativa, correttiva o innovativa del modello. Esse sono:
- Innovazioni legislative sia del D. Lgs. 231/2001 che delle norme richiamate dal catalogo dei reati in essere
- Modifiche organizzative della società sia in relazione all'organigramma che al ciclo attivo o passivo, o alle modalità di business
- Azioni di remediation e/o implementazione in corso e non concluse
- Fine tuning del modello in corso.

L'OdV può essere contatto al seguente indirizzo email *organismodivigilanza@gruppoitalcer.it*

Area sensibile	Riferimento normativo
Sicurezza sul lavoro	Art. 25-septies
Reati ambientali	Art. 25-undecies
Reato societari	Art- 25-ter
Reati tributari	Art. 25-quinquiesdeces
Riciclaggio e autoriciclaggio	Art. 25-octies
Truffa ai danni dello stato	Art. 24
Corruzione e concussione	Art. 25
Trattamento dei dati sensibili	Art. 24-bis
Cybersecurity	Art. 24-bis



Monitoraggio dei presidi
Il monitoraggio dei presidi avviene con controlli di terzo livello sulle funzioni di secondo livello (Compliance e Risk).
La funzione Compliance raccoglie e aggiorna la matrice tra normativa applicabile e processi del presidio.
La funzione Risk valuta il rischio inerente oggettivo e poi rivaluta il rischio rispetto alla Compliance con l'eventuale produzione di un piano di rimedio.
La funzione di Audit controlla l'esecuzione del remediation plan oltre al funzionamento dei processi di Compliance e di Risk Management e fornisce flussi informativi all'ODV.

7
Gli strumenti di prevenzione

Per quanto riguarda il codice etico ed il codice disciplinare, gli stessi sono visibili ai seguenti link:
www.ceramicarondine.it/it/corporate-e-compliance
eliosceramica.com/corporate-and-compliance

Per quanto riguarda invece il piano di formazione, come detto in premessa, trattandosi di elemento costitutivo fondamentale del modello organizzativo, deve avere le caratteristiche di «formazione continua».

Il nostro Modello organizzativo prevede la raccolta delle seguenti informazioni in merito:

- Piano formativo
- Curriculum dei formatori e relativo contratto
- Contenuto di corsi
- Materiale dei corsi
- Elenco dei partecipanti
- Test di autoapprendimento relativo a ciascun partecipante
- Feedback da parte di ciascun partecipante.

Alle stesse informazioni si può accedere dall'organigramma per ciascuna persona che ha partecipato.
La formazione continua è diretta a divulgare le novità legislative e le modifiche al modello. Essa può quindi essere mirata alla parte del personale dipendente interessata dalle predette novità.

8
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, ovvero 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, sono 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 link: italcer.integrityline.com

FOLLOW US

WWW.GRUPPOITALCER.IT