ITALCER GROUP

DESIGN SURFACES

MODELLO ORGANIZZATIVO
EX D. LGS. 231/2001

Linee guida per l'implementazione ed il funzionamento

ELIOS ceramica

CERAMICA Rondine

BOTTEGA

Premessa

Il 14 dicembre 2021 il Consiglio di Amministrazione di Italcer S.p.A. («**Italcer**» o la «**Società**») ha approvato l'adozione del Modello di Organizzazione, Gestione e Controllo (di seguito anche «Modello Organizzativo») 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.

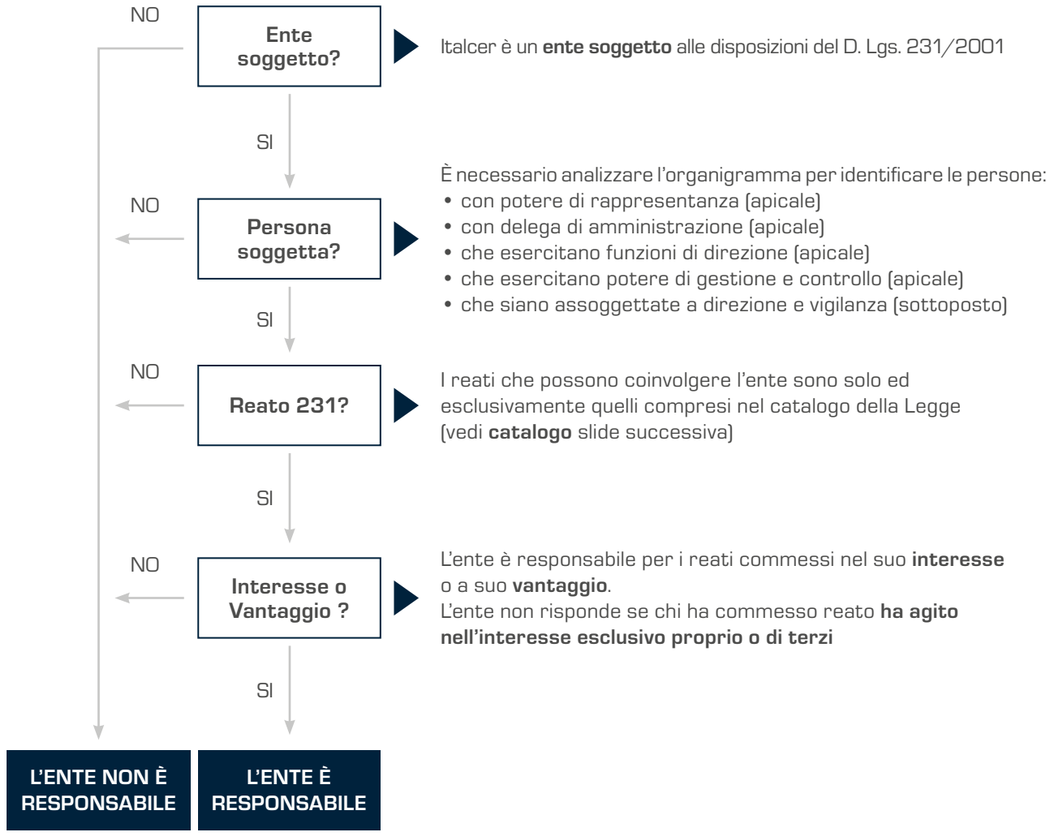
Il presente documento, pubblicato sul sito web della Società, ha il precipuo scopo di illustrare le linee guida che hanno ispirato l'adozione e l'attuazione del Modello stesso, attraverso l'approfondimento dei relativi passaggi applicativi.

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 (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. 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**

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 Organizzativo

PREVENZIONE:

Formazione continua

Codice etico

Codice disciplinare

Policy e procedure

Organismo di Vigilanza (ODV)

ATTIVITÀ A BASSA COMPLESSITÀ

CONTROLLO:

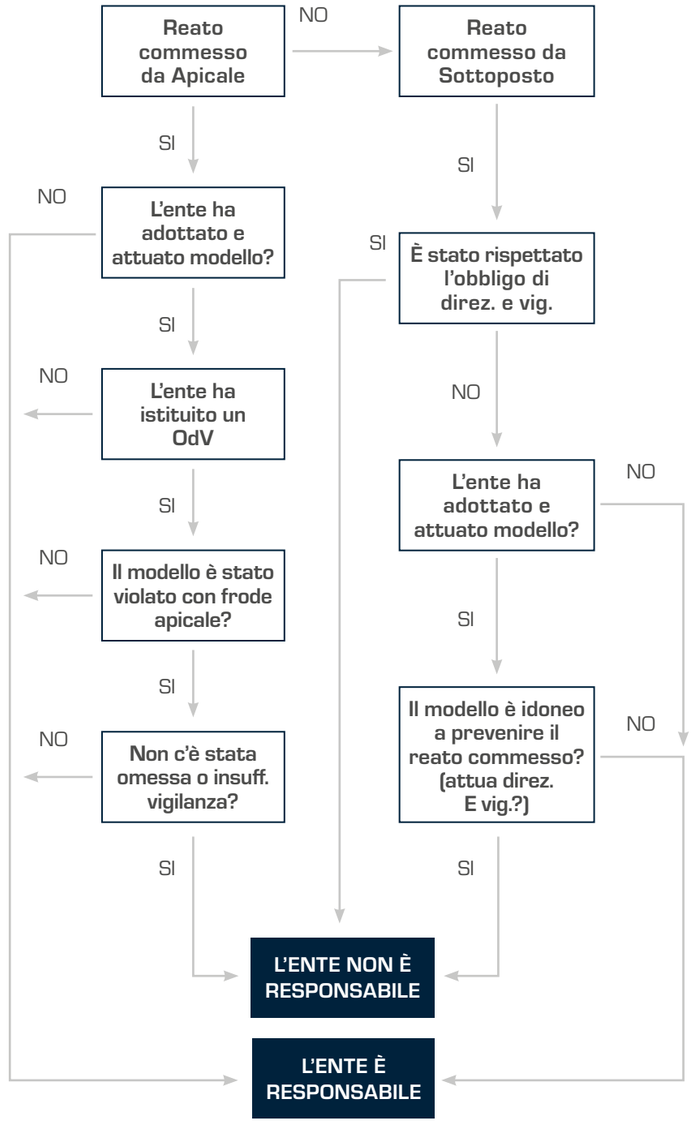
Flusso informativo periodico all'ODV e all'Internal Audit sullo stato di efficienza e di funzionamento del Modello Organizzativo

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 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:

COMPANY PROFILING

Il **Company Profiling**, che ha l'obiettivo di conoscere e fotografare l'azienda, evidenziando, con un'appropriata analisi il piano di azione per l'adozione e l'attuazione del Modello Organizzativo.

- 1. INQUADRAMENTO GENERALE
- 2. ASSESSMENT SUL PERSONALE
- 3. ASSESSMENT SUL GRUPPO DI APPARTENENZA
- PIANO D'AZIONE

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 ciascun'area.

- 1. SETUP ORGANIZZATIVO
- 2. SETUP DEI PRESIDI DI CONTROLLO
- 3. SETUP DEGLI STRUMENTI DI PREVENZIONE

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 DEI FLUSSI DEL MODELLO ORGANIZZATIVO
- 2. MONITORAGGIO DELLE NOVITÀ LEGISLATIVE
- 3. MONITORAGGIO DEI CAMBIAMENTI ORGANIZZATIVI

3
Il company profiling

COMPANY PROFILING

- 1. INQUADRAMENTO GENERALE
- 2. ASSESSMENT SUL PERSONALE
- 3. ASSESSMENT SUL GRUPPO DI APPARTENENZAREATI
- 4. PIANO D'AZIONE

Il **Company Profiling** ha l'obiettivo di conoscere e fotografare l'azienda, evidenziando, con un'appropriata analisi, il piano di azione per la progettazione ed implementazione del Modello Organizzativo.

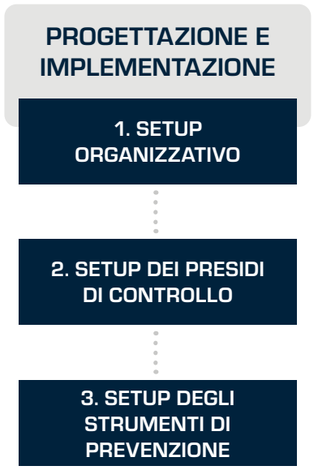
Il processo è condotto tramite l'utilizzo di procedure predefinite che mirano specificamente a:

1. Predeterminare in base alle informazioni ed ai parametri aziendali quali sono le aree di potenziale rischio ai fini della commissione dei reati 231.

2. Fotografare il personale dipendente con la creazione di un organigramma dinamico che raccoglie tutte le informazioni disponibili e che soprattutto è predisposto per collegare ciascuna figura in esso contenuta alle condotte sensibili delle aree di rischio. All'interno dell'organigramma è anche possibile disegnare sub organigrammi riferiti ai processi sensibili.

3. Fotografare il Gruppo di imprese controllate da Italcer al fine di controllare le correlazioni esistenti ai fini 231 in tema di:
   - Governance
   - Contratti di prestazioni di servizi
   - Contratti di distacco di personale
   - Contratti di finanziamento
   - Contratti di cessione di beni.

4
Progettazione e Implementazione



Nella fase **Progettazione e Implementazione** del Modello Organizzativo, la nostra Società ha creato un repository di documenti e processi correlati atti a prevenire e controllare la commissione dei reati 231. In particolare:

1. nella fase di Setup Organizzativo è stato costruito l'organigramma interattivo ed il sociogramma con le interrelazioni e sono stati attivati nel repository in modo da fungere da sistema connettore dei diversi processi aziendali;
2. nella fase di Setup dei presidi di controllo (cap. 4.1 infra) sono stati valutati il rischio inerente ed il rischio residuo di ciascuna area sensibile per valutare sia il grado di criticità che le azioni da porre in essere per raggiungere un livello di compliance pari al 100%;
3. nella fase di setup degli strumenti di prevenzione e controllo sono stati messi a punto il piano di formazione e la relativa esecuzione dello stesso, nonché il Codice Etico ed il Codice Disciplinare.

La parte cosiddetta «**parte generale**» del Modello Organizzativo, nel rispetto della classica definizione delle linee guida di Confindustria, è stata realizzata con un repository normativo dedicato, a cui è possibile far rinvio via ipertesto da tutte le parti del Modello Organizzativo, che richiamano una norma specifica o qualsiasi elemento regolatorio di riferimento.

4.1 Setup dei presidi di controllo

A seguito del Company Profiling sono state individuate le seguenti aree a rischio potenziale:

Sicurezza sui luoghi di lavoro
Sicurezza ambientale
Sicurezza informatica
Reati contro la pubblica amministrazione
Reati tributari e societari

La valutazione sarà condotta annualmente per valutare l'allargamento o la riduzione della casistica.

Per ciascuna area sensibile è stata condotta una valutazione del rischio inerente come indicato nelle slides che seguono.

4.1.2 Setup dei presidi di controllo: metodologia di valutazione del rischio

VALUTAZIONE RISCHIO COMMISSIONE REATO			DANNO			
			Nullo	Lieve	Medio	Grave
			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 >=12

La metodologia classica prevede la valutazione del rischio in base al combinarsi di due variabili:

- la probabilità che si verifichi un incidente
- il danno che procura il verificarsi dell'incidente.

La probabilità, come meglio spiegato in appresso, dipende dalla casistica specifica di ciascuna area tenuto conto delle varie sfaccettature del rischio; il danno, invece, viene valutato sotto un triplice aspetto:

- impatto economico e finanziario
- impatto reputazionale
- impatto sull'operatività e sulla business *continuity.*

In base alle valutazioni specifiche, che sono illustrate di seguito, le aree a sensibilità elevata in Italcer sono risultate:

- **Sicurezza sui luoghi di lavoro**
- **Sicurezza ambientale**

Area a sensibilità media la **Sicurezza Informatica.**

Aree a sensibilità moderata ma comunque da tenere in evidenza:

- Reati contro la pubblica amministrazione
- Reati societari e tributari.

4.1.3 Setup dei presidi di controllo: metodologia di valutazione del rischio (un'altra visione)

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.

4.1.4 Setup dei presidi di controllo: valutazione del rischio sicurezza sul lavoro

Per il calcolo delle probabilità sono stati presi in esame alcuni parametri chiave quali, a titolo esemplificativo:

- Numero dipendenti
- Composizione dipendenti per categoria
- Composizione dipendenti per mansione
- Anzianità media degli impianti
- Anzianità media dei tecnici
- Numero impianti
- Dimensione media impianti
- Grado di automazione della produzione
- Turni di produzione

Per ogni impianto è stata poi valutata la rischiosità in base alla casistica **INAIL**:

- Rischio legato ad agenti biologici
- Rischio legato ad agenti cancerogeni
- Rischio legato ad agenti chimici
- Rischio legato ad agenti fisici
- Rischio legato ad atmosfere esplosive
- Rischio legato ad attrezzature di lavoro
- Rischio legato a fattori di ergonomia
- Rischio legato all'impiego di nanotecnologie
- Rischio legato a polveri e fibre
- Rischio elettrico

4.1.5 Setup dei presidi di controllo: GAP analysis area sicurezza sul lavoro

La GAP *analysis* (per singolo impianto) è stata invece impostata anzitutto sulle prescrizioni di Legge di cui al D. Lgs. 81 del 2008, con specifiche check list di controllo e la possibilità di collegare ciascuna singola risposta ad un documento specifico o ad un processo specifico.

In secondo luogo, si è fatto riferimento alle prescrizioni e linee guida dell'**INAIL**, in relazione alle singole fattispecie di rischio.

Nel caso specifico della nostra Società, la GAP *analysis* ha evidenziato una ragionevole corrispondenza a tutte le prescrizioni di legge anche in linea con le seguenti certificazioni ISO che sono state rilasciate per singolo impianto:

- ISO 9001
- ISO 14001
- ISO 45001
- ISO 50001

Per quanto riguarda il *leit motiv* del nostro Modello Organizzativo, ovvero la correlazione di ogni attività di prevenzione e controllo al personale della Società, l'area di rischio sicurezza sul lavoro presenta un proprio specifico organigramma interattivo, avente le caratteristiche funzionali dell'organigramma principiale e ad esso collegato come estrapolazione specifica.

Il *remediation plan* che ne è scaturito e che verrà tenuto costantemente sotto controllo, costituisce elemento dinamico del Modello Organizzativo.

4.1.6 Setup dei presidi di controllo: valutazione del rischio sicurezza ambientale

Per il calcolo delle probabilità sono stati presi in esame alcuni parametri chiave quali, a titolo esemplificativo:

- Numero dipendenti
- Composizione dipendenti per categoria
- Composizione dipendenti per mansione
- Anzianità media sugli impianti
- Anzianità media dei tecnici
- Numero impianti
- Dimensione media impianti
- Grado di automazione della produzione
- Turni di produzione
- Età media degli impianti

Per ogni impianto è stata poi valutata la rischiosità in base alla classificazione dell'ARPA nazionale:

- Inquinamento suolo
- Inquinamento sottosuolo
- Inquinamento idrico
- Inquinamento dell'aria
- Smaltimento rifiuti

4.1.7 Setup dei presidi di controllo: GAP analysis area sicurezza ambientale

La GAP *analysis* (per singolo impianto) è stata, invece, impostata anzitutto sulle prescrizioni di Legge di cui al D. Lgs. 152 del 2006, su specifiche check list di controllo e sulla possibilità di collegare ciascuna singola risposta ad un documento o ad un processo specifico.

In secondo luogo, si è fatto riferimento alle prescrizioni per i controlli AIA o AUA (a seconda dell'obbligo) e secondariamente alle linee guida dell'ARPA nazionale, in relazione alle singole fattispecie di rischio.

Nel caso specifico della nostra Società, la GAP *analysis* ha evidenziato una ragionevole corrispondenza a tutte le prescrizioni di legge anche in linea con le seguenti certificazioni ISO che sono state rilasciate per singolo impianto:

- ISO 9001
- ISO 14001
- ISO 45001
- ISO 50001

Anche per questa area sensibile, come per l'area Sicurezza sul Lavoro, è stato creato uno specifico organigramma interattivo, avente le caratteristiche funzionali dell'organigramma principiale e ad esso collegato come estrapolazione specifica.

Il *remediation* plan che ne è scaturito e che verrà tenuto costantemente sotto controllo, costituisce elemento dinamico del Modello Organizzativo.

4.1.8 Setup dei presidi di controllo: valutazione del rischio sicurezza informatica e GAP analysis

Per il calcolo delle probabilità, a fronte di una mappatura del sistema informativo sia fisica che logica, nonché delle funzionalità esistenti in azienda, viene valutata la probabilità inerente che si verifichi una delle seguenti minacce di *incident* previste dall'autorità europea per il controllo della pirateria informatica ENISA:

- Ransomware
- Malware
- Cryptojacking
- Attacchi alla posta elettronica (e-mail)
- Attacchi ai dati
- Attacchi web
- Disinformazione
- Misinformazione

La GAP *analysis* nel caso di Italcer è stata condotta con l'ausilio di un primario consulente a livello nazionale che, a fronte di specifici test, è stato in grado di predisporre tutte le misure di prevenzione e di controllo dei possibili *incident* come sopra indentificati. **Italcer si è, quindi, dotata di un sistema qualitativamente avanzato di prevenzione e controllo delle condotte dei suoi manager e sottoposti in tema di potenziali reati informatici.**

4.1.9 Setup dei presidi di controllo: le aree a rischio moderato

Per le aree sensibili a rischio moderato (reati tributari, societari, contro la PA e reati finanziari in genere) è stata comunque eseguita la misurazione del rischio inerente e la GAP *analysis*.

In questo caso, ispirandosi alle linee guida dell'ANAC, alle linee guida della Agenzia delle Entrate nonché alle Leggi in vigore ed ai principi contabili nazionali ed internazionali.

Apposite *policy* e linee guida aiuteranno ad eseguire le procedure aziendali in modo dinamico, cioè predisponendo specifiche attività di controllo sulle policy stesse, sulla loro attuazione nonché sulla loro osservanza, e collegando sempre ogni policy alle relative figure di riferimento in qualità sia di esecutori che di controllori.

Di seguito alcune policy e procedure (oltre a quelle predisposte per le aree più sensibili) che costituiscono e costituiranno l'ossatura di riferimento:

- Procedura nomine
- Procedura formazione bilanci e report
- Procedura assesment tributari
- Procedura selezione fornitori
- Procedura AML clienti e fornitori
- Policy conflitti di interesse
- Policy anticorruzione
- Formalizzazione del ciclo attivo e passivo con interazione dinamica ed evidenza dei sottocicli

4.2 Setup degli strumenti di prevenzione

L'azienda ha predisposto i seguenti strumenti di prevenzione:

1. Codice etico: visibile sui vari siti aziendali tra cui anche: **www.ceramicarondine.it/static/core/attachments/codice_etico.pdf**

2. Codice disciplinare: visibile per estratto al seguente link: **https://www.ceramicarondine.it/media/filer_public/93/3c/933cfe35-3fa7-4f18-a0d9-890b69c8ccaf/italcer_codice_disciplinare_estratto.pdf**

3. Formazione continua: su questo aspetto Italcer si è attivata con corsi di formazione in presenza a tutti i dipendenti della Società. Sono stati eseguiti test di autovalutazione ed è stata emesso un attestato di frequenza. Tutti gli atti sono consultabili nel repository su cui si basa il Modello Organizzativo, sia nella partizione dedicata all'*education,* che come informazioni specifiche di ciascun dipendente partecipante.

   Il piano di formazione prevede un richiamo annuale per estendere la formazione ai nuovi assunti oltre che per trasferire eventuali modifiche esogene o endogene al Modello Organizzativo

   All'emissione delle policy, delle procedure o di qualsiasi altro documento esecutivo, si procede con la relativa formazione al personale coinvolto.

4.3 Setup dei processi di monitoraggio

Il nostro Modello Organizzativo prevede tre tipologie di monitoraggio:

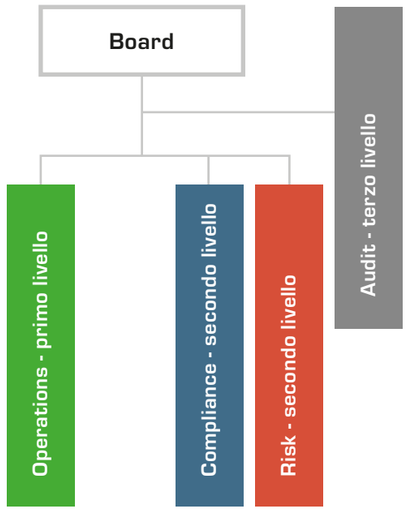
1. Monitoraggio dei flussi. Proveniente dal *repository* documentale ed alimentato dai piano di rimedio, nonché dai *task* gestiti da ciascun singolo utente per l'esecuzione delle attività necessarie a raggiungere il massimo livello di compliance. Sono disponibili sia report parziali che totali, sia cartacei che digitali.

2. Un monitoraggio periodico eseguito dalla funzione Compliance per verificare che non vi siano novità legislative che riguardano il D. Lgs. 231/2001. Novità che vengono subito recepite dal repository, ma che potrebbero comunque comportare revisioni dell'impianto di prevenzione e controllo specifico di qualche area sensibile.

3. Un monitoraggio periodico per verificare eventuali cambiamenti organizzativi, che potrebbero implicare modifiche nei protocolli di prevenzione e controllo.

Gli esiti dei monitoraggi sono comunque inviati all'Organismo di Vigilanza.

4.3.1 Setup dei processi di monitoraggio: la funzione di controllo



La funzione di controllo interna 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 interna di risk management and compliance, individuata in una figura manageriale, anche membro interno dell'Organismo di Vigilanza

Controlli di terzo livello eseguiti dalla funzione Audit a diretto riporto del Consiglio di Amministrazione, che avrà diretto accesso al repository documentale del Modello Organizzativo.

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, 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 seguente link: **https://italcer.integrityline.com**

ITALCER GROUP

DESIGN SURFACES

FOLLOW US

WWW.GRUPPOITALCER.IT