CompliWare

Il processo per l’implementazione e la manutenzione dei modelli organizzativi 231

CompliWare

Indice

1. Implementazione del Modello: generazione dei processi di costruzione
2. Implementazione del Modello: setup degli strumenti di prevenzione
3. L’output cartaceo tradizionale
4. L’output digitale
5. il Risk Assessment: il contenuto
6. il Risk Assessment: definizioni
7. il Risk Assessment: l’impiego dell’AI
8. il Risk Assessment: l’impiego dell’AI – rappresentazione grafica
9. il Risk Assessment: analisi preliminare (primo livello) delle aree di rischio
10. il Piano di rimedio
11. Manutenzione e aggiornamento periodico del Modello

1. Implementazione del Modello: generazione dei processi di costruzione

CompliWare

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.

prosegue a pagina successiva

2. Implementazione del Modello: setup degli strumenti di prevenzione

CompliWare

da pagina precedente

Codice etico

Il Codice Etico 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 la società ha scelto volontariamente di adottare e rendere pubblici, come concreta espressione dei loro 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 Modello organizzativo 231 ed è prevalentemente svolta in aula con sistemi di valutazione per l'apprendimento.

3. L’output cartaceo tradizionale

CompliWare

Parte generale

Contiene i principi fondamentali del sistema di gestione del rischio, tra cui il quadro normativo di riferimento, gli obiettivi del modello, 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 Modello
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 dall'azienda 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

4. L’output digitale

Tutta la documentazione della Compliance integrata, passata e presente, archiviata e disponibile nella suite di CompliWare.

Archiviazione statica per ricerca, visione e stampa di metadati relativi a:

- Validità residua di tutti i documenti aziendali
- Documenti in corso di revisione per area di rischio
- Organigrammi storici e attuali e relativi documenti
- Sociogrammi storici e attuali e relativi documenti
- Qualsiasi altro documento (sia 231 che non) caricato nel contesto della compliance

Archiviazione dinamica per ricerca, visione e stampa di metadati relativi a:

- Soggetti responsabili della prevenzione e controllo
- Soggetti collegati alle aree di rischio e ai relativi processi
- Soggetti responsabili della gestione dei processi
- Soggetti che hanno in carico la revisione dei documenti
- Work in progress della gestione documentale
- Collegamenti dinamici tra documenti esplicativi di processi o policy e persone coinvolte
- Collegamenti dinamici tra i processi dei rapporti infragruppo e persone coinvolte

5. il Risk Assessment: il contenuto

- Identificazione dei **rischi potenziali**
- Definizione di rischio **inerente** e di rischio **residuo,** di **probabilità** di accadimento e di **impatto** sull'azienda
- Metodologie di **valutazione** dei rischi
- **Classificazione** delle **aree sensibili** in base al livello di rischiosità
- Misurazione del **GAP** vs una Compliance 100%
- Determinazione delle **azioni di rimedio**
- Definizione di un **remediation plan**
- **Implementazione** e **monitoraggio**
- La **metodologia applicativa** utilizzata per il caso specifico (**ente** per il quale si progetta il modello)
- **Risk assessment** per singola area di rischio individuata per **l'ente** specifico
- Il **piano di rimedio dell'ente** specifico

6. il Risk Assessment: 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.

7. il Risk Assessment: l'impiego dell'AI

L'impiego dell'AI consente di sintetizzare tutte le già menzionate attività in un **unico processo** attraverso i seguenti sottoprocessi consequenziali:

1. **Creazione** delle **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**.

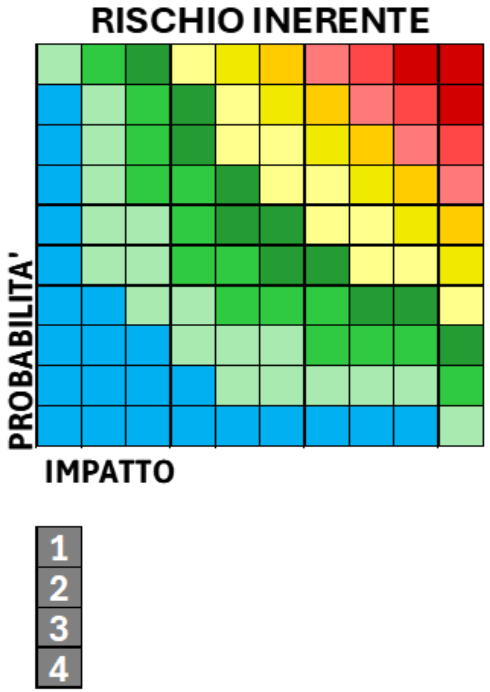
L'algoritmo elabora i dati su quattro livelli:

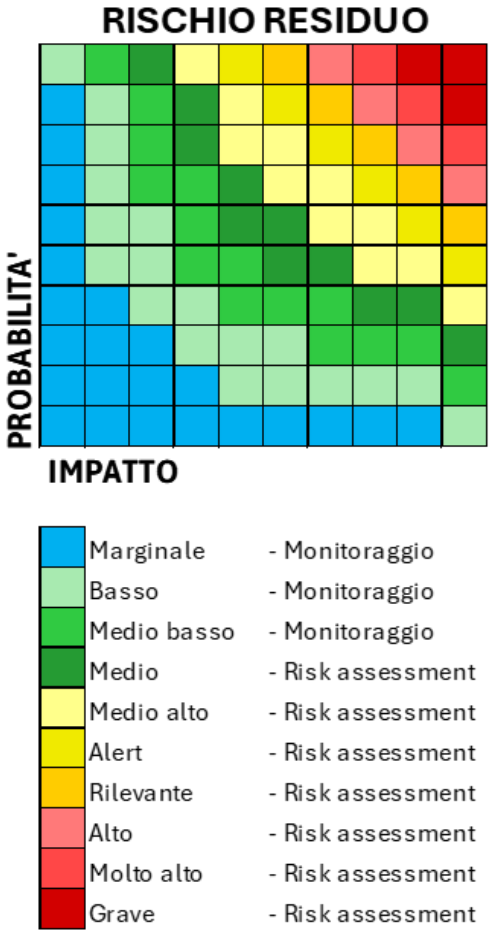
- livello 1: sulla **fattispecie** di reato e le sue condotte
- livello 2: su **contesti** della fattispecie di reato individuati dall'algoritmo (da 1 a N contesti)
- livello 3: per ogni contesto, misurazione di **probabilità** e **impatto** dell'evento con riferimento al **rischio inerente** (da 1 a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

8. il Risk Assessment: l'impiego dell'AI – rappresentazione grafica

Livello 1	Livello 2	Livello 3	Livello 4
Reato	**Contesto**	**Rischio inerente**	**Rischio residuo**
	Contesto 1	Probabilità (da 1 a 10)	Probabilità (da 1 a 10)
		Impatto (da 1 a 10)	Impatto (da 1 a 10)
	Contesto 2	Probabilità (da 1 a 10)	Probabilità (da 1 a 10)
		Impatto (da 1 a 10)	Impatto (da 1 a 10)
	Contesto N	Probabilità (da 1 a 10)	Probabilità (da 1 a 10)
		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





9. il Risk Assessment: analisi preliminare (primo livello) delle aree di rischio

Articolo	Categoria di reato	Descrizione	Azione
Art. 24	Indebita percezione di erogazioni, truffa ai danni dello Stato, frode informatica	Reati commessi per ottenere indebitamente fondi pubblici o ingannare lo Stato con mezzi fraudolenti, incluse truffe e frodi informatiche ai danni della P.A.	Rimedio
Art. 24-bis	Delitti informatici e trattamento illecito di dati	Comprende accesso abusivo a sistemi informatici, diffusione di malware, frode informatica con furto d'identità digitale.	Rimedio
Art. 24-ter	Delitti di criminalità organizzata	Reati commessi nell'ambito di associazioni criminali, mafiose, finalizzati a ottenere il controllo di attività economiche, o trarre vantaggi illeciti mediante intimidazione, corruzione o violenza.	Rimedio
Art. 25	Concussione, induzione indebita e corruzione	Abusi di potere da parte di pubblici ufficiali per ottenere indebiti vantaggi economici o favori.	Rimedio
Art. 25-bis	Falsità in monete, carte di pubblico credito e valori di bollo	Falsificazione e utilizzo fraudolento di monete, carte di pagamento e valori bollati.	N/A
Art. 25-bis.1	Delitti contro l'industria e il commercio	Frode in commercio, vendita con segni mendaci, usurpazione di titoli di proprietà industriale.	Monit.
Art. 25-ter	Reati societari	False comunicazioni sociali, abuso di potere, infedeltà patrimoniale e ostacolo alla vigilanza.	Monit.
Art. 25-quater	Delitti con finalità di terrorismo	Reati legati a organizzazioni terroristiche, atti di violenza per destabilizzare lo Stato o istigazione a tali atti.	N/A
Art. 25- quater 1	Reati di mutilazione degli organi genitali femminili	Pratiche di mutilazione degli organi genitali femminili.	N/A
Art. 25-quinquies	Delitti contro la personalità individuale	Tratta di persone, riduzione in schiavitù, sfruttamento della prostituzione minorile e pedopornografia.	N/A
Art. 25-sexies	Abusi di mercato	Manipolazione del mercato, abuso di informazioni privilegiate, insider trading.	N/A
Art. 25-septies	Omicidio colposo e lesioni colpose gravi o gravissime con violazione delle norme sulla sicurezza sul lavoro	Reati derivanti dalla violazione delle norme di sicurezza nei luoghi di lavoro.	Rimedio
Art. 25-octies	Ricettazione, riciclaggio, impiego di denaro di provenienza illecita, autoriciclaggio	Attività di occultamento e reimpiego di fondi o beni ottenuti illegalmente.	Monit.
Art. 25-octies.1	Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori	Frodi informatiche e utilizzo fraudolento di strumenti di pagamento digitali.	N/A
Art. 25-novies	Delitti in materia di violazione del diritto d'autore	Duplicazione abusiva di software, diffusione non autorizzata di opere tutelate.	N/A
Art. 25-decies	Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria	Induzione o pressione per far rilasciare dichiarazioni false alla magistratura.	Rimedio
Art. 25-undecies	Reati ambientali	Inquinamento, gestione illecita dei rifiuti, violazione delle norme sugli scarichi e sull'uso del suolo.	Rimedio
Art. 25-duodecies	Impiego di cittadini di paesi terzi il cui soggiorno è irregolare	Assunzione e sfruttamento di lavoratori stranieri irregolari.	Rimedio
Art. 25-terdecies	Razzismo e xenofobia	Condotte discriminatorie e incitamento all'odio basate su razza, etnia, nazionalità o religione.	N/A
Art. 25-quaterdecies	Frode in competizioni sportive	Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e utilizzo di apparecchi vietati per il gioco d'azzardo.	N/A
Art. 25-quinquiesdecies	Reati tributari	Dichiarazioni fraudolente, occultamento di documenti contabili e indebite compensazioni fiscali.	Rimedio
Art. 25-sexiesdecies	Contrabbando	Evasione di dazi doganali, importazione illegale di merci.	N/A
Art. 25-septiesdecies	Delitti contro il patrimonio culturale	Danno o furto di beni culturali e storici, falsificazione di opere d'arte.	N/A
Art. 25-duodevicies	Riciclaggio di beni culturali e devastazione di beni e paesagg.	Reimpiego di beni culturali illecitamente acquisiti o distruzione di patrimonio culturale.	N/A

10. 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.

La suite CompliWare fornisce report appropriati sia per l’Organismo di vigilanza che per l’Internal audit

11. Manutenzione e aggiornamento periodico del Modello

CompliWare

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

Variazioni nelle informazioni di contesto (ciclo attivo, passivo, ciclo di produzione, diversificazioni, differenziazione, apertura nuovi mercati ecc.)

Nuovo piano di audit

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