



FARETE

6-7 settembre 2023
BolognaFiere



Padiglione 16-18
Ingresso Nord

LA COMPLIANCE AZIENDALE

Dai sistemi di gestione, al modello di organizzazione, gestione e controllo (D.Lgs. 231/01) sino al «whistleblowing» ed alla «responsabilità sociale» d'impresa.

1. **DEFINIZIONE – I settori della Compliance aziendale**
2. **STANDARDS ISO E SISTEMI GESTIONALI**
3. **CORPORATE CRIMINAL LIABILITY E D.LGS. 231/01 – Il Modello Organizzativo (MOG) 231**
4. **MODELLO ORGANIZZATIVO E SISTEMI GESTIONALI**
5. **WHISTLEBLOWING**
6. **CORPORATE SUSTAINABILITY. Verso nuovi obblighi per le imprese**
7. **CORPORATE SOCIAL RESPONSIBILITY & CORPORATE SUSTAINABILITY**
8. **MOG 231 & ESG/CSR. A confronto**
9. **MOG 231 & ESG/CSR. Verso la Compliance integrata**

1. COMPLIANCE - Definizione

COMPLIANCE AZIENDALE



Termine utilizzato in **ambito aziendale** con il significato di «**rispetto**» e «**conformità**» a:

- ❖ **Standard tecnici** (e.g. standard relativi alla qualità di beni e servizi o standard per la certificazione del bilancio);
- ❖ **legge** (e.g. il rispetto delle norme per la tutela della salute e sicurezza sul lavoro, dell'ambiente, dei diritti umani, etc.);
- ❖ **best practices** (e.g. modalità di condotta raccomandate da associazioni di categoria o a organismi nazionali e internazionali).

ma.... «Compliance» significa anche adottare **un sistema organizzato di regole di condotta, procedure e presidi di controllo**

I settori della Compliance Aziendale



2. Gli Standards UNI ISO



L'**International Organization for Standardization (ISO)** è un'organizzazione internazionale, i cui componenti sono enti di normazione nazionali, **che definisce degli standard internazionali di condotta «volontari»**, utilizzati da aziende e altre organizzazioni e riconosciuti a livello globale.

Gli **Standards UNI ISO** si riferiscono ad una **serie di norme «tecniche» internazionali che stabiliscono requisiti, linee guida e *best practice* in diversi ambiti**, come la gestione della qualità, l'ambiente, la sicurezza delle informazioni, la responsabilità sociale, la gestione dell'energia, etc.

2. Gli Standards UNI ISO e Sistemi gestionali

Pianificare e Valutare (Plan - Assessment)

- Stabilire gli obiettivi e valutare il rischio

Fare (Do)

- Predisporre i processi e presidi di controllo

Verificare (Check)

- Monitorare

Migliorare (Act)

- Azione di miglioramento

2. Standards ISO e Compliance

Standard UNI ISO = COMPLIANCE TECNICA

Gli Standard UNI ISO:

- ❖ definiscono le **regole tecniche alle quali l'impresa si deve «conformare»** - «su base volontaria» - per raggiungere gli obiettivi definiti dallo standard di riferimento.
- ❖ individuano **una metodologia per la «costruzione» di un sistema di gestione** (i.e. un complesso di procedure coordinate tra di loro).
- ❖ richiedono la predisposizione di una serie di **procedure dedicate** allo scopo indicato dallo Standard UNI ISO.
- ❖ Attraverso **l'attività di monitoraggio** continuo consentono di rilevare le criticità del sistema di gestione ed elaborare (ed attuare) azioni di miglioramento continuo tiraggio.



Gli **STANDARD UNI ISO** rappresentano l'**antesignano dei sistemi di compliance dell'impresa**

3. Responsabilità «penale» dell'impresa

La Corporate Criminal Liability - USA

❖ Elkins Act – 1903

Legge federale degli US che dispone che *"le azioni e le omissioni realizzate da un rappresentante che opera per conto dell'ente"*, debbano *«essere attribuite all'ente, che ne subirà conseguenze penali»*.

❖ Leading case: New York Central & Hudson River Railroad Co. v. United States, 212 U.S. 481 - 1909

Statuisce la **piena responsabilità penale delle persone giuridiche**, anche per quelle fattispecie caratterizzate dall'elemento soggettivo. → **Superamento del principio «societas delinquere non potest»**.

❖ Foreign Corrupt Practices Act (FCPA) 1977

E' una **normativa statunitense volta a sanzionare le imprese statunitensi il cui personale si renda responsabile di atti o condotte corruttive al fine di acquisire commesse e/o affari in paesi stranieri**.

❖ US Compliance Programs

Il **Dipartimento di Giustizia americano**, in collaborazione con la SEC, ha pubblicato nel corso del tempo delle **linee guida sulle condotte che le società statunitensi devono seguire** (cd. **«Compliance Program»**) individuandone gli **elementi fondanti** (le **minimum best practices**) con l'obiettivo di rispettare le normative anti-corrruzione di riferimento. E' previsto tra l'altro che **la supervisione delle policies anti-corrruzione sia svolta da una «struttura dedicata»** (*«Specific Individual/s – Compliance Officer»*).

3. Il Decreto Legislativo 231/01

B) D.Lgs. 231/2001 → la Compliance «sbarca» in Italia

- ❖ Il **D.lgs. 8 giugno 2001 n. 231 («Decreto 231»)** contiene la «**Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità**».

Genesis: Legge 29 settembre 2000, n. 300: legge di ratifica delle seguenti convenzioni:

- ☐ Convenzione PIF del 26 luglio 1995 sulla tutela degli interessi finanziari della Comunità Europea;
- ☐ Convenzione relativa alla lotta contro la corruzione di funzionari delle Comunità Europee o degli Stati membri dell'Unione Europea (Bruxelles 26 maggio 1997);
- ☐ Convenzione OCSE sulla lotta alla corruzione di pubblici ufficiali stranieri (Parigi 17 dicembre 1997):

Le Convenzioni richiedono di perseguire non solo la persona fisica responsabile della corruzione, ma anche **le imprese coinvolte nel reato**.

- ❖ Il **Decreto 231 stabilisce che l'ente è responsabile dei reati commessi nel suo interesse e/o vantaggio da coloro che rivestono funzioni «apicali» o da persone sottoposte alla direzione/vigilanza delle persone «apicali»**
- ❖ **L'IMPRESA ASSUME UN RUOLO DI RESPONSABILITA' «SOCIALE» NELLA CONDOTTA DEL PROPRIO PERSONALE, DIRETTA AD EVITARE CONDOTTE CONTRA LEGEM**

3. I casi di esclusione della responsabilità ex Decreto 231

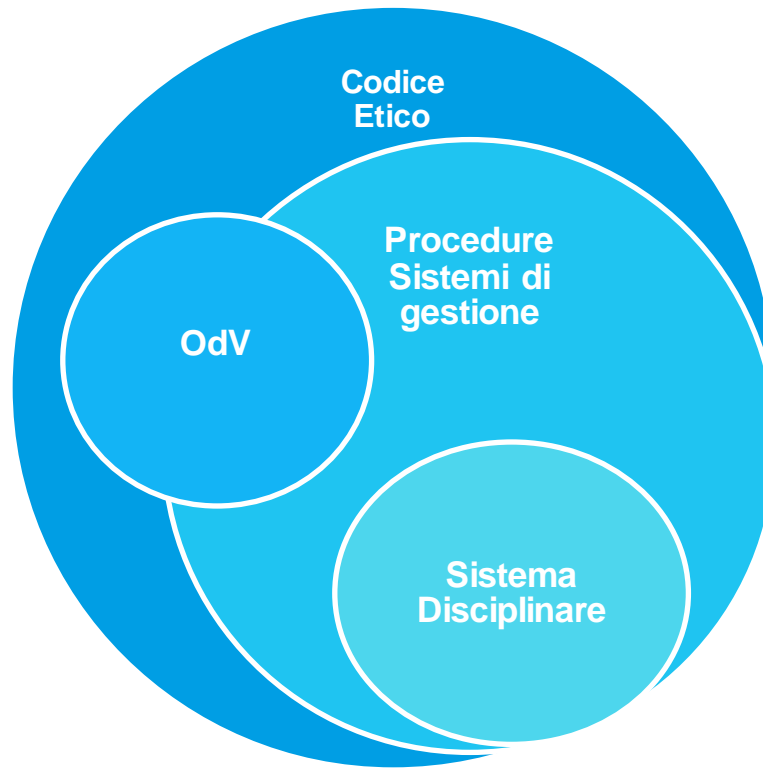
Anche in caso di commissione di uno dei reati previsti dal D.lgs. 231/01 è prevista una forma specifica di **esonero della responsabilità dell'ente, purché sia provato che:**

- ❖ l'organo dirigente della società ha adottato, prima della commissione del fatto, **un modello di organizzazione (il «Modello Organizzativo») idoneo a prevenire la commissione dei Reati Presupposto;**
- ❖ il compito di vigilare sul funzionamento e l'osservanza del Modello Organizzativo, nonché di segnalare all'organo dirigente della Società la necessità di aggiornamento del Modello Organizzativo, è stato affidato a un **organismo indipendente («ODV»);**
- ❖ l'autore del reato (che svolge funzioni di rappresentanza, amministrazione, direzione della Società o è un sottoposto di soggetto che riveste tali funzioni) ha agito **eludendo fraudolentemente** il Modello Organizzativo;
- ❖ **non vi sia stata omessa o insufficiente vigilanza.**



L'adozione del Modello Organizzativo non è obbligatoria, ma in caso di commissione di un Reato Presupposto è il solo modo per la Società (in presenza di tutti presupposti sopra indicati) di andare esente dalle sanzioni altrimenti previste a suo carico.

3. Il Modello di Organizzazione e Gestione «MOG»)



Il **Modello Organizzativo** è un sistema complesso formato dai seguenti diversi componenti;

- ❖ **Codice Etico**
- ❖ **Procedure e sistemi gestionali**
- ❖ **Organismo di vigilanza**
- ❖ **Sistema disciplinare**

3. La sequenza degli interventi per il MOG

L'adozione di un Modello Organizzativo richiede il compimento di una serie di **attività richieste dal D.lgs. 231/2001** e condotte sulla base delle **Linee Guida** redatte dalle Associazioni di Categoria (es. ANCE, Confindustria) e della **best practice consolidatasi in materia**.



N.B. IL MODELLO ORGANIZZATIVO DEVE ESSERE COSTRUITO “SU MISURA” IN RELAZIONE ALLE SPECIFICHE ATTIVITA’ A RISCHIO DELL’ENTE

4. MOG e Sistemi gestionali

Aspetti di **correlazione** tra **Modello Organizzativo 231** e **Sistemi Gestionali**:

Modello Organizzativo 231	Sistemi Gestionali
Codice Etico	Politica della Qualità/Sicurezza/Ambiente
Risk Assessment	Contesto dell'organizzazione – Valutazione del rischio
Organigrammi e mansionari – Poteri autorizzativi	Leadership – Ruoli nell'organizzazione
Procedure (manuali od informatiche) – Presidi di controllo	Attività operative
Comunicazione e formazione al personale	Supporto (Risorse umane)
Monitoraggio	Valutazione delle performance

4. MOG e Sistemi gestionali

Aspetti di **distinzione** tra **Modello Organizzativo 231** e **Sistemi Gestionali**:

Modello Organizzativo 231	Sistemi Gestionali
Funzione: Prevenzione del reato	Funzione: Miglioramento dell'attività di impresa rispetto al sistema gestionale prescelto
Sistema disciplinare	[N/A]
Monitoraggio: Audit interni - OdV	Monitoraggio: Audit interni – certificazione esterna



- ❖ I Sistemi gestionali **NON** comprendono l'**intero spettro delle aree a rischio reato** ai sensi del D.Lgs. 231/2001.
- ❖ Taluni Sistemi gestionali **NON** contemplano la **mappatura di aree che invece sono a rischio reato** ai sensi del D.lgs 231/2001 (e.g. si veda l'ISO 9001 e l'area delle procedure amministrative e contabili).

5. Whistleblowing

L'evoluzione normativa in tema di *whistleblowing*



L. 190/2012
Introduzione del
whistleblowing nel
settore pubblico

L. 179/2017
Estensione del
whistleblowing al
settore privato e
ampliamento delle
tutele nei confronti
del «segnalante»

**Direttiva UE
2019/1937**
Armonizzazione
degli ordinamenti
nazionali in
relazione alla
protezione delle
persone che
segnalano violazioni
del diritto dell'UE

D. Lgs. 24/2023
Recepimento
nell'ordinamento
italiano delle
disposizioni
contenute nella
Direttiva UE

**+ Linee Guida
ANAC, efficaci dal
15/07/2023**

Forniscono indicazioni
e principi di cui gli
enti pubblici e privati
possono tener conto
per i propri canali e
modelli organizzativi
interni.

Il D.lgs. 24/2023 («Decreto Whistleblowing»)

- abroga la disciplina nazionale previgente in materia di *whistleblowing* concentrando in un unico testo normativo il regime di protezione dei soggetti che segnalano condotte illecite («whistleblowers») di cui siano venuti a conoscenza in un contesto lavorativo
- si pone l'obiettivo di garantire un approccio bilanciato tra la protezione del whistleblower e la salvaguardia delle imprese da utilizzi distorti o abusivi di questo strumento, per minimizzare il rischio di gravi danni reputazionali

5. Whistleblowing

Ambito di applicazione soggettivo

Enti interessati

- Società che abbiano impiegato nell'ultimo anno almeno **50 lavoratori subordinati** a tempo determinato o indeterminato
- Società che abbiano adottato un **Modello di Organizzazione, Gestione e Controllo** anche se hanno impiegato **meno di 50 dipendenti**
- Società appartenenti **a settori speciali** che rientrano nell'ambito di applicazione degli atti dell'UE (si veda Allegato al Decreto Whistleblowing) in materia di servizi, prodotti e mercati finanziari, prevenzione del riciclaggio e finanziamento del terrorismo, sicurezza dei trasporti e tutela dell'ambiente, anche se hanno impiegato **meno di 50 dipendenti**

Chi può segnalare?

- Lavoratori **subordinati** e **autonomi**
- **Collaboratori** o **fornitori** di beni e servizi
- **Liberi professionisti** o **consulenti**
- **Volontari** e **tirocinanti**, retribuiti e non retribuiti
- **Azionisti** e persone con **funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza**
- Soggetti che siano venuti a conoscenza di una violazione nell'ambito del contesto lavorativo anche **prima dell'instaurazione del rapporto di lavoro** (durante il processo di selezione o in altre fasi precontrattuali), durante il **periodo di prova** o **successivamente allo scioglimento** del rapporto di lavoro

5. Whistleblowing

Quali violazioni possono essere segnalate?

Illeciti amministrativi, contabili, civili e penali

Condotte illecite rilevanti ai sensi del D.Lgs. 231/2001 o violazioni del Modello Organizzativo

Atti od omissioni che ledono gli interessi finanziari dell'UE

Illeciti che rientrano nell'ambito di applicazione degli atti dell'UE o nazionali*

Atti od omissioni riguardanti il mercato interno (nonché in materia di concorrenza e aiuti di stato e di imposte sulle società)

*nello specifico: appalti pubblici; servizi, prodotti, e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente; radioprotezione e sicurezza nazionale; sicurezza degli alimenti e dei mangimi e salute e benessere degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi.

6. Corporate Sustainability. Verso nuovi obblighi per le imprese

NFRD (*Non-Financial Reporting Directive*)

Direttiva 2014/95/UE

- Recepita in Italia dal D. Lgs. 30 dicembre 2016, n. 254
- Introduce obblighi di comunicazione di informazioni di carattere non finanziario da parte di talune imprese e di taluni gruppi di grandi dimensioni

CSRD (*Corporate Sustainability Reporting Directive*)

Direttiva (EU) 2022/2464

- In fase di recepimento da parte degli Stati membri (luglio 2024)
- Introduce obblighi di rendicontazione societaria di sostenibilità per le grandi imprese, anche non quotate, e le PMI (ad eccezione delle micro-imprese) quotate

Proposal for a CSDDD (*Corporate Sustainability Due Diligence Directive*)

COM(2022) 71 final

- Introduce obblighi di due diligence per talune imprese di grandi dimensioni rispetto agli impatti negativi sui diritti umani e sull'ambiente, effettivi o potenziali, che incombono alle società nell'ambito delle loro attività, delle attività delle loro filiazioni e delle attività nella catena del valore

7. Corporate Social Responsibility & Corporate Sustainability

Nuovo ruolo e nuovi obblighi per le organizzazioni.
Origini ed evoluzione del concetto di Responsabilità Sociale d'Impresa (RSI)

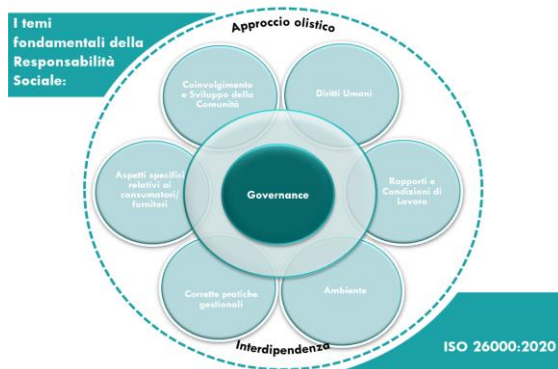
Le elaborazioni della dottrina americana

- «Social Responsibilities of the Businessman» (Bowen 1953)
- The Pyramid of CSR (Carroll 1979;1991)
- Triple bottom line (Elkington 1997)

Il contributo degli organismi internazionali

- Linee Guida OCSE per le imprese multinazionali
- Dichiarazione tripartita OIL di principi sulle imprese multinazionali e la politica sociale
- UN Global Compact
- Principi guida ONU su imprese e diritti umani

Gli Standard volontari



L'approccio della Commissione europea

- «Integrazione volontaria delle preoccupazioni sociali ed ecologiche delle imprese nelle loro operazioni commerciali e nei loro rapporti con le parti interessate» (Libro Verde 2001)
- «Responsabilità delle imprese per il loro **impatto sulla società**. Per soddisfare pienamente la loro responsabilità sociale, le imprese devono avere in atto un processo per **integrare le questioni sociali, ambientali, etiche, i diritti umani e le sollecitazioni dei consumatori** nelle loro operazioni commerciali e nella loro strategia di base in stretta collaborazione con i rispettivi interlocutori, con l'obiettivo di: fare tutto il possibile per **creare un valore condiviso** tra i loro proprietari /azionisti e gli altri loro soggetti interessati e la società in generale; **identificare, prevenire e mitigare i loro possibili effetti avversi**» (Strategia rinnovata dell'UE per il periodo 2011-14 in materia di responsabilità sociale delle imprese)

7. Corporate Social Responsibility & Corporate Sustainability

IL CONTRIBUTO DEL SETTORE PRIVATO AGLI OBIETTIVI DI SVILUPPO SOSTENIBILE

Definire e attuare percorsi di sostenibilità all'interno delle organizzazioni



L' Agenda 2030 delle Nazioni Unite e gli Obiettivi di Sviluppo Sostenibile (*Sustainable Development Goals – SDGs*) rappresentano un importante strumento per le imprese che vogliono definire strategie, programmi e obiettivi per l'analisi e il miglioramento delle loro performance sotto il profilo della sostenibilità ambientale, sociale e di governance.

Per l'integrazione della sostenibilità all'interno del modello di business aziendale sono essenziali:

HOW?

Individuazione delle tematiche ambientali, sociali e di governance (ESG) rilevanti per l'impresa

Valutazione degli impatti ESG, attuali e potenziali, correlati all'attività d'impresa e analisi dei relativi rischi/opportunità

Definizione di un piano strategico per il raggiungimento di specifici obiettivi di miglioramento

Sviluppo e monitoraggio di indicatori di prestazione per la verifica dello stato di raggiungimento dei risultati

Il **coinvolgimento degli stakeholder (Stakeholder Engagement)** è un processo fondamentale per la corretta definizione e l'efficace attuazione di un percorso di sostenibilità, in quanto permette all'impresa di:

Mappare i propri portatori di interesse

Comprenderne le istanze e aspettative

Comunicare in modo trasparente informazioni utili

Integrare i processi decisionali e strategici

Contribuire alla creazione di valore condiviso

8. MOG 231 & ESG/CSR a confronto

ASPETTI DI DISTINZIONE	
Finalità	Il MOG 231 ha lo scopo di prevenire la commissione dei reati-presupposto contemplati dal D. Lgs. 231/01, mentre la definizione di politiche e strategie di sostenibilità mira all' integrazione degli aspetti ambientali, sociali e di governance all'interno del modello e della strategia di business , al fine di generare valore condiviso per l'organizzazione e per i suoi stakeholder
Ambito	Gli aspetti di rilevanza delle strategie di sostenibilità sono potenzialmente estesi ad ogni ambito di operatività dell'organizzazione, nonché ampliati alla catena del valore, anziché limitati alla potenziale rilevanza penale di condotte e attività riconducibili all'elenco tassativo dei reati-presupposto di cui al D. Lgs. 231/01
ASPETTI DI CORRELAZIONE E ANALOGIA	
Volontarietà	Attualmente, l'adozione del MOG 231e/o la definizione di politiche e strategie ESG & CSR rappresenta una sceita volontaria per le organizzazioni (ma si vedano NFRD e CSRD)
Tematiche rilevanti	Si riscontra una parziale sovrapposizione tra tematiche e ambiti di operatività dei due sistemi (es. tutela dell'ambiente, eticità della condotta d'impresa)
Presidii di controllo	All'interno del sistema di controlli interni dell'organizzazione, può aversi coincidenza tra presidii di controllo implementati ai fini 231 e strumenti di gestione e monitoraggio degli impatti ESG (es. in materia HSE, anti-corruzione, ecc)
Reati 231	
Reati commessi nei rapporti con la PA	<div><div> 12 CONSUMO RESPONSABILE</div><div> 16 PACE, GIUSTIZIA E ISTITUZIONI SANE</div></div> <div>GRI 205 (Anticorruzione)</div>
Reati ambientali	<div><div> 6 ACQUA PULITA E SERVIZI IGIENICO-SANITARI</div><div> 9 IMPRESE, INNOVAZIONE E INFRASTRUTTURE</div><div> 11 CITTÀ E COMUNITÀ SOSTENIBILI</div><div> 12 CONSUMO RESPONSABILE</div></div> <div>GRI 301 (Materiali); GRI 302 (Energia); GRI 303 (Acqua ed effluenti); GRI 304 (Biodiversità); GRI 305 (Emissioni); GRI 306 (Rifiuti)</div>
Omicidio e lesioni	<div><div> 3 SALUTE E BENESSERE</div><div> 8 LAVORO DIGNITOSO E CRESCITA ECONOMICA</div><div> 10 RIDUZIONE DELLE DISUGUAGLIANZE</div></div> <div>GRI 403 (Salute e sicurezza sul lavoro)</div>

9. MOG 231 & ESG/CSR. Verso la Compliance integrata

- Definire una **Politica aziendale integrata** (principi etici per la prevenzione dei reati + diffusione di una cultura della sostenibilità)
- Strutturare un **sistema integrato di gestione dei rischi** (attività **risk assessment congiunte, trasversali e per processi + integrazione del sistema di presidi di controllo interno e delle procedure aziendali** per la contestuale individuazione, valutazione e gestione, per ciascun processo aziendale, dei rischi-reato e dei rischi ESG)
- Individuare potenziali **sinergie e integrazioni** ulteriori **a livello organizzativo-gestionale** (es. canali di segnalazione)
- Stabilire adeguati **flussi informativi** tra le funzioni aziendali coinvolte (Compliance Manager, Sustainability Manager, Internal Audit, RSGL), nonché con i diversi organi di controllo (OdV, CS)

PROMUOVERE L'INTEGRAZIONE TRA I DUE SISTEMI SIGNIFICA:

Razionalizzare l'impiego di risorse

Aumentare l'efficacia e l'efficienza delle attività

Evitare sovrapposizioni di ruoli, duplicazioni di adempimenti, verifiche e azioni correttive

Facilitare la condivisione di informazioni

Ridurre il rischio di potenziali incoerenze, controlli non ottimizzati o mancanza di presidi

...MA ANCHE **VALORIZZARE LA COMPLIANCE 231**

Il sistema di controllo interno implementato ai fini 231 (anche) come **strumento di supporto al perseguimento di obiettivi ESG**, quantomeno in termini di **analisi e gestione dei rischi** di impatti negativi (es. area HSE)

L'adozione e l'efficace attuazione del MOG 231 contribuiscono all'**adeguatezza dell'assetto organizzativo dell'impresa** in ottica ESG quale **fattore di governance**

Grazie

per l'attenzione!

Avv. Alberto Bertuzzo:

alberto.bertuzzo@studiopirola.com

Dott.ssa Silvia Monaldi:

silvia.monaldi@studiopirola.com



MAKES IT EASY

Compliance

Settembre 2023



- Presentazioni
- Compliance
- Obiettivi
- Analisi del Rischio
- Le Origini dalla Qualità ad oggi
- Compliance in Maticmind (Responsabilità)
- Compliance in Maticmind - Certificazioni
- Compliance in Maticmind (SGI)
- Compliance in Maticmind – Modello 231 ed ESG
- Punti di riflessione

agenda





MATICMIND S.p.A. (www.maticmind.it)

Leader in Italia nel settore della ICT System Integration, progetta, integra e gestisce soluzioni tecnologiche innovative, grazie a competenze specialistiche in tutte le aree dell'Information & Communication Technology (Cyber Security, Data Center & Cloud, Digital Workplace, Networking, Enterprise Applications, Digital Automation Solutions, Servizi e Soluzioni 5G)

- **Dipendenti Maticmind:** >800
- **Ricavi (Maticmind):** 287 milioni di euro (2021)
- **Società del Gruppo:** Fibermind, Cloudmind, SIO, SIND, ITI (sarà integrata dal 1° ottobre)
- **Sedi:** Milano, Torino, Padova, Modena, S. Fiorentino (FI), Roma, Ciampino (RM), Napoli, S. Spirito (BA), S. Giovanni La Punta (CT)
- **Clienti:** Finance, Enterprise, Healthcare, Education, Public Sector (PAC e PAL), Telco Provider

Giorgio Pavarani

Direttore Compliance, Sustainability, Risk Management & Safety in Maticmind S.p.A.

In precedenza:

- *Direttore Acquisti, Logistica, Safety&Facility, Compliance dal 01/04/2017 al 30/07/2023 in Maticmind S.p.A.*
- *Responsabile Ingegneria di Offerta in Maticmind S.p.A.*
- *Responsabile Area Tecnica Nord in Maticmind S.p.A.*
- *Responsabile Acquisti Commerciali in Wind Telecomunicazioni S.p.A.*
- *Responsabile Acquisti ICT in Wind Telecomunicazioni S.p.A.*
- *Responsabile Acquisti ICT in Infostrada S.p.A.*
- *Responsabile Acquisti ICT in Italtel SIT S.p.A.*



E' un insieme di attività organizzative ed operative volte al rafforzamento dei presidi aziendali atti ad assicurare la piena osservanza delle normative riguardanti l'attività svolta e le relazioni con le Parti Interessate (Stakeholder).

Con il termine «Compliance», tra le possibili definizioni, si intende così quel tessuto organizzativo, guidato da una Funzione/Direzione, che garantisce la continua conformità agli standard e alle normative vigenti, mediante un «sistema di regole», che l'azienda ha deciso di adottare per funzionare in modo ottimizzato, costruito su una adeguata e concreta gestione della riduzione del rischio.

Tra le normative generali che generalmente sono fatte rientrare nell'ambito del controllo vi sono:

- Standard Internazionali ISO, tra le più frequenti: ISO9001:2015, ISO14001:2018, ISO14064:2019, ISO27001:2013, ISO2001:2019, ISO45001:2018, ISO26001;
- Safety - Dlgs. 81/2008 sulla "Sicurezza sul Lavoro e Tutela della Salute sul Posto di Lavoro".
- Dlgs. 231/01 sulla "Responsabilità Amministrativa delle Persone Giuridiche"
- Privacy e Protezione dei Dati Personali (GDPR)

Le ragioni che spingono una organizzazione a sviluppare un efficace Sistema di Compliance sono da ricercare:

- Governo dell'azienda: processi chiari e ben descritti, le norme rispettate e gli indicatori facilmente rilevabili;
- Disporre di un **Sistema di Gestione Integrato** - ovvero politiche, processi, procedure, istruzioni operative, ruoli e responsabilità per supportare il lavoro suggerendo metodi e strumenti «standard» univoci per tutto il personale.
- Garanzia di un Modello Organizzativo 231 valido, aggiornato ed efficace;
- Lo sviluppo del principio della Sostenibilità, sul quale tutto il mondo industriale e commerciale è ormai obbligato a tendere: processi e prodotti più efficienti sono meno inquinanti (inquinamento fisico, chimico) quindi alla fine meno costosi per l'impresa ed i suoi Clienti;
- Le certificazioni ISO, oltre ad essere un «obbligo» per il miglioramento stanno assumendo una rilevanza «commerciale» assoluta: permettono la qualificazione in Albo Cliente e soprattutto regalano «punti» di qualificazione nelle gare, essenziali quando l'aggiudicazione sul prezzo si batte in pochi punti percentuali di differenza.

Oggi un buon sistema di Compliance rappresenta un vantaggio che, finalmente, viene percepito come necessario dalla organizzazione, dai Clienti, dagli azionisti, quale potente sistema di riduzione dei rischi.



L'Analisi del Rischio, termine ormai presente nel lessico comune, è lo strumento con il quale costruire il «sistema delle regole» il cui contesto è determinato dal momento aziendale, la dinamica della normativa, i processi sensibili esposti a reati o non conformità.

Ad ogni rischio individuato o «entrante» deve corrispondere un «rischio uscente» che viene ridotto tramite politiche e procedure adeguate («sistema delle regole») mantenuto attraverso:

- Aggiornamento dei modelli organizzativi e delle procedure che descrivono i processi;
- Piano di audit per verificare l'osservanza del sistema di regole;
- Report delle attività e flussi informativi per tenere aggiornati organi supervisor sui risultati ottenuti o su eventi di non conformità con carattere di rilevanza;
- Canali di comunicazione al giusto livello e contenuto;
- Elevata attenzione per le certificazioni ISO conseguite e loro mantenimento;
- Attenta valutazione per lo sviluppo di nuove certificazioni (benefici vs. costi).



Le pratiche aziendali legate all'aderenza alle norme UNI EN ISO a partire dalla ISO 9001, apparsa nel tessuto industriale italiano a fine anni '80, rappresentano l'origine di quello oggi chiamiamo «Compliance»,

L'aderenza a queste norme «non cogenti» costrinse le organizzazioni a comportamenti che migliorarono sensibilmente, ed in modo continuo, sia la qualità del prodotto venduto (si pensi ad esempio al tracciamento di un componente dal costruttore all'utilizzatore) che la conoscenza operativa dei processi e delle fasi di lavoro, soprattutto nelle catene del servizio (uno fra tutti la documentazione delle righe del software).

Nei successivi decenni lo svilupparsi delle norme, anche verso gli aspetti cogenti, ha determinato un sistema di valutazione per le imprese a garanzia della bontà dei processi di una organizzazione.

Negli ultimi vent'anni con l'affacciarsi di nuovi decreti (sicurezza, etica ed anticorruzione, ecc.) e l'introduzione nelle norme del concetto di risk management (vedi ISO9001:2000 o «vision») l'insieme delle regole si è evoluto in un «Sistema Integrato della Qualità», fondamentali ad esempio nella qualificazione dei Fornitori.

E' su questa «dorsale» che si costruiscono le parti complementari di compliance etica (d.lgs. 231), ambientale, sociale e governance (ESG e CSR), che alla fine devono sfociare nella sostenibilità etica ed ambientale del business.



Obblighi di legge

D.lgs. 231:2001, Testo Unico sulla Sicurezza 81/08, Regolamento (UE) 679/2016 e D.lgs. 196:2003, Direttiva 2022/2464/EU in materia di corporate sustainability.

Governo della ISO 9001:2015, della ISO/IEC 20000-1:2018, della ISO/IEC 27001:2013 (in coordinamento con il CISO), della ISO 45001:2018, ISO14001, ISO14064.

Standard ISO

Contrattualistica

Sensibilità sui contratti (**modelli standard**) e valutazione dei rischi nella catena di fornitura (**valutazione e qualificazione dei Fornitori**), impatti su D.lgs. 231:2001 e Testo Unico 81/08, Regolamento (UE) 679/2016 e D.lgs. 196:2003.

Indicatori di Compliance (Ambiente, Sociali, Governance, sistemi etici)

Indicatori

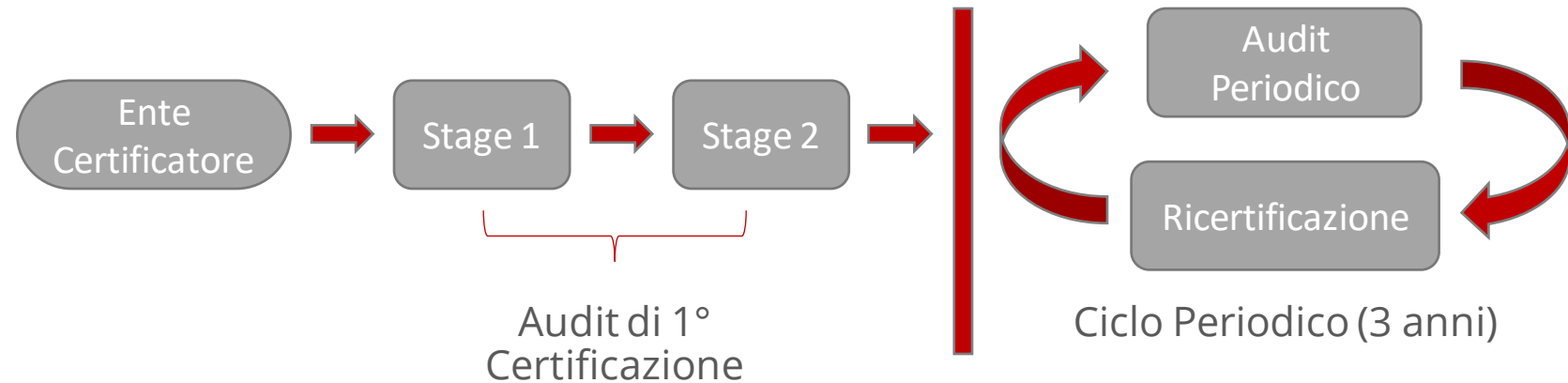
Assessment / Audit

Audit di terze parti, assesment per qualificazioni (ESG/CSR, privacy, B.C. Security, ecc.)



La certificazione è una valutazione, condotta da un ente terzo indipendente, allo scopo di verificare che il sistema delle regole strutturato dall'Organizzazione sia aderente e rispetti i requisiti stabiliti dalla norma.

Percorso di Certificazione



Benefici della Certificazione

- Migliorare la reputazione dell'Organizzazione e la fiducia nei suoi confronti
- Rispettare i requisiti aziendali, legali, contrattuali e normativi
- Ottenere un giudizio indipendente sullo stato di sicurezza del SGI
- Ridurre perdite economiche e reputazionali associate a violazioni di dati
- Valore aggiunto di distinzione nel proprio mercato di riferimento
- Riduzione dei rischi informatici e dei relativi impatti negativi
- Fidelizzazione dei propri Clienti



Le norme internazionali ISO sono elaborata dagli organismi di standardizzazione (ISO e IEC) allo scopo di fornire i requisiti tecnici ed organizzativi per stabilire, attuare, mantenere e migliorare in modo continuo un Sistema di Gestione. Maticmind ha sviluppato e conseguito:

- **ISO9001:2015**

Lo standard internazionale richiede l'adozione di un processo per l'attuazione delle Attività (UNI EN ISO 9001:2015). E' la prima certificazione ottenuta, aggiornata nel 2017 che determina la realizzazione di un Sistema di Gestione della Qualità.

- **ISO27001:2013**

Seconda certificazione acquisita da Maticmind (Maggio 2019) che vede come perimetro di riferimento le strutture organizzative del Network Operation Center (NOC) e Security Operation Center (SOC).

- **ISO45001:2018**

Terza certificazione in ordine cronologico ottenuta ad Ottobre 2019. Riguarda tutte le sedi Maticmind ed è stato determinante per la gestione dell'emergenza SarsCov2. E' tra le norme quella che coinvolge maggiormente il personale Maticmind e in particolare i PM, più sensibili ai rischi amministrativi e penali, con la procedura di Gestione della Sicurezza nei Contratti di Appalto

- **ISO20000-1:2018**

Acquisita nell'Aprile del 2020, relativa al Service Management ha molti punti "di contatto" con le altre due certificazioni ISO9001 e ISO27000 e prevede anch'essa l'adozione di un processo per le Attività Operative più articolato ed ampio rispetto a quello richiesto dalla ISO9001.



■ ISO14001:2018

E' la quinta certificazione acquisita a marzo 2023: La norma richiede la realizzazione di procedure di gestione e quantificazione energetica e di emissioni che diano luogo a un sistema di gestione ambientale

■ ISO14064-1:2018

E' la sesta certificazione acquisita a marzo 2023. Permette di quantificare le emissioni di GHG al fine di attuare delle politiche di Carbon Management e comunicare il proprio impegno in tema di sostenibilità ambientale ai propri stakeholder



Un Sistema di Gestione è l'insieme delle politiche, delle procedure e dei processi (il sistema delle regole) stabiliti da allo scopo di raggiungere gli obiettivi definiti, quali la qualità ad esempio dei prodotti e servizi forniti, la sicurezza e salute dei lavoratori, la sicurezza delle informazioni e la qualità dei servizi erogati.

Il **Sistema di Gestione Integrato** è il frutto dell'insieme di più Sistemi corrispondenti agli obiettivi indicati, che unisce il Sistema di Gestione della Qualità (SGQ) a quello della Salute e Sicurezza sul Lavoro (SGSL), per la Sicurezza delle Informazioni (SGI) ed altri (ad esempio il Service Management).

Tale Sistema si ispira alla struttura definita dagli standard ISO/IEC, denominata **High Level Structure (HLS)**, che specifica i requisiti per stabilire, attuare, mantenere e migliorare in modo continuo un Sistema di Gestione nel contesto di un'Organizzazione.

Fondamentale è la comunicazione: disponibilità di informazioni (procedure, documenti, comunicazioni, dati, ecc.) tramite Portali aggiornati ed affidabili di facile ed immediata consultazione.



- Il Modello ed il Codice Etico sono stati redatti nel 2017 ed approvati dal CDA;
- Nel corso del 2018 è stato implementato il Modello Organizzativo in accordo con l'OdV: accettazione e formazione dipendenti (che è aggiornata periodicamente), comunicazioni alle parti interessate, procedura whistleblowing, pianificazione degli audit;
- Nel 2019 l'OdV, con il supporto della Funzione Qualità, ha condotto gli audit mensili a tutte le Direzioni;
- Nel 2020 è stato aggiornato il MOG (prima revisione) per adempiere agli aggiornamenti normativi intercorsi dal 2017. OdV ha inoltre condotto audit alla funzione Safety per la gestione dell'emergenza epidemiologica;
- Nel 2021 è stato revisionato il Modello Organizzativo (seconda revisione) adeguandolo alle variazioni dell'organizzazione Maticmind. OdV ha condotto audit alla funzione Safety per l'emergenza epidemiologica ed alle altre Direzioni;
- Nel 2022 è stato aggiornato il documento dell'Analisi del rischio/reato (prima revisione);
- Nel 2023 sono state adeguate alla norma anticorruzione e catalogo reati 231 le Procedure più sensibili del Sistema Integrato della qualità (SGI), che hanno condotto alla terza revisione del MOG ed alla seconda revisione della Analisi dei Rischi / Reato e sarà condotta una sessione di formazione agli apicali. E' inoltre stata aggiornata la procedura di whistleblowing (seconda revisione): nella seconda metà dell'anno verrà scelta e resa disponibile la piattaforma per le segnalazioni
- Nel 2024 è in programma lo sviluppo delle tematiche di sostenibilità e responsabilità sociale d'impresa e di rendicontazione in ambito ESG (Environment, Social, Governance) e CSR (Corporate Social Responsibility). Inoltre è pianificata una pesante revisione dell'Analisi dei Rischi / Reato, che dovrà raccogliere sia gli aggiornamenti normativi che le variazioni organizzative nei processi dell'Azienda.



La progettazione di un Sistema di Compliance deve seguire la natura dell'Impresa (industriale, servizi, commerciale), dai prodotti trattati e dal loro impatto ambientale, dalla dimensione ed dai Clienti (pubblici, privati, business o consumer) e deve essere rapportato con i benefici che esso può dare.

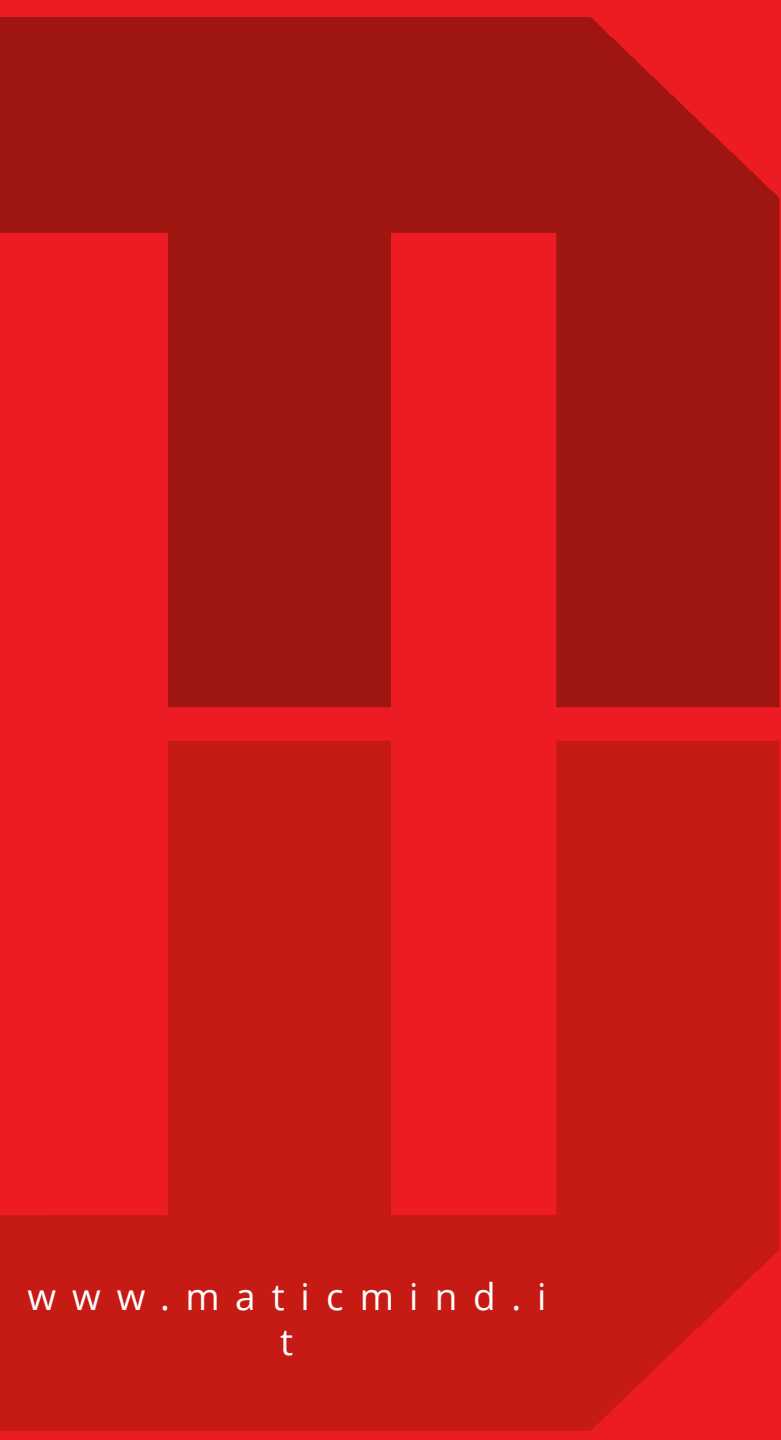
Un Sistema di Compliance deve pertanto seguire una attenta dialettica propedeutica circa l'opportunità della sua realizzazione, del suo livello di approfondimento e soprattutto del suo mantenimento, implicando esso importanti costi diretti ed indiretti da confrontare con fatturato e margini, poiché:

- Impegna sensibili costi diretti verso gli organismi di certificazioni e di vigilanza;
- Richiede profonde conoscenze su aspetti in continuo aggiornamento che richiedono collaborazioni con società di consulenza o studi legali;
- Richiede una organizzazione dedicata con risorse esperte, anche in tematiche manageriali, non facilmente reperibili ed in continuo aggiornamento;
- Impegna tutte strutture organizzative in ripetuti audit o di sessioni di lavoro, «distringendole» dalle attività.

Un Sistema di Compliance deve essere una vera leva di competitività e non diventare una «sovrastuttura» che consuma risorse senza dare evidenti vantaggi.



GRAZIE PER L'ATTENZIONE



DATA CENTER



COLLABORATION



NETWORK



APPLICATIONS

SECURITY

www.maticmind.it