COMPLIANCE AZIENDALE

Formazione 4.0 -

Cos'è

Compliance è la conformità delle attività aziendali alle disposizioni normative, ai regolamenti, alle procedure ed ai codici di condotta, che possiamo identificare con il termine "Norme", siano esse cogenti come volontarie.

La ***Compliance aziendale*** è quindi un'attività preventiva che si preoccupa di prevenire il rischio di non conformità dell'attività aziendale alle Norme, suggerendo ove si riscontrino disallineamenti le più opportune soluzioni.

La ***Funzione Compliance*** è la struttura organizzativa cui è affidato il compito di:

- prevenire i disallineamenti tra le procedure aziendali e l'insieme delle regole interne ed esterne all'azienda
- assistere le strutture aziendali nell'applicazione delle Norme
- predisporre interventiformativi per adeguare le procedure interne dei dipendenti e dei collaboratori alle Norme
- coordinare e garantire l'attuazione degli adempimenti richiesti dalle Norme
- risolvere situazioni di discordanza tra le Norme in vigore e le specifiche realtà operative dell'azienda
- assicurare le relazioni con le Autorità ed Organi di Controllo interni ed esterni

La normativa

Il decreto legislativo 231/01 ha introdotto il concetto di responsabilità amministrativa delle imprese per reati commessi da amministratori, manager o dipendenti, collegando ad esse pesanti sanzioni pecuniarie o interdittive.

Tale disposizione prevede infatti l'attribuzione di alcuni tipi di reati non più solo alle persone fisiche che hanno commesso l'illecito, ma anche e soprattutto alle persone giuridiche quali ad esempio le società per cui lavorano.

I destinatari di tale Decreto sono gli enti dotati e non di personalità giuridica quali, ad esempio, Spa, Srl, Sapa, Snc, Sas, associazioni, cooperative, fondazioni, enti economici sia privati che pubblici e più in generale tutte le imprese organizzate in forma societaria.

La normativa è esclusa solo per le imprese individuali.

I principali reati previsti da tale decreto sono quelli verso le Pubbliche Amministrazioni (quali truffa, concussione, corruzione, indebita percezione di erogazioni pubbliche ,ecc) e la maggior parte dei reati societari (falso in bilancio, false comunicazioni sociali, aggiotaggio, ecc.). Vi sono inoltre reati legati ad eversione e terrorismo, delitti contro la persona, falsificazione di monete e reati transnazionali. La tendenza, comunque, è quella di inserire in futuro all'interno del Decreto anche reati in materia ambientale, di sicurezza sul lavoro e sfruttamento della manodopera.

L'impresa può essere esentata dalla responsabilità (art. 6 del D.Lgs. 231/01) se fornisce la prova di aver efficacemente adottato, prima della commissione del fatto, modelli di organizzazione e gestione idonei a prevenire reati della specie di quello verificatosi, di vigilare sull'osservanza di tali modelli e che il reato è stato attuato da un soggetto che abbia eluso fraudolentemente i modelli di organizzazione e controllo.

Da una lettura combinata di quanto previsto dall'art. 2392 del Codice Civile che tratta la responsabilità degli amministratori e dall'art. 6 del D.Lgs. 231/01, è possibile affermare che gli amministratori potranno evitare la responsabilità civile per i danni causati alla società e quella penale per omesso impedimento dei reati, solo adottando ed efficacemente attuando i modelli di organizzazione e gestione previsti dal D.Lgs. 231/01.


CERTIFIED
ISO
9001:2008
COMPANY
D.Lgs.81/08
Compliance
Aziendale
privacy
HACCP

I modelli di organizzazione , gestione e controllo

La legge non prevede alcuna obbligatorietà di dotarsi di un modello organizzativo idoneo a prevenire i reati.

Tuttavia, l'adozione di un modello organizzativo valido ai sensi della 231/2001 comporta una serie di vantaggi significativi per la società o l'ente.

I vantaggi che derivano dall'introduzione di un modello di organizzazione e gestione, possono essere molteplici quali ad esempio:

-evitare l'applicazione delle sanzioni pecuniarie o interdittive

-ridurre il rischio di illeciti

-ridurre la possibilità di esclusione da appalti e subappalti pubblici

-tutelare l'investimento dei soci e degli azionisti in relazione al danno economico dovuto all'attuazione dei reati di cui sopra

-tutelare l'immagine dell'azienda

-aumentare il vantaggio competitivo dell'azienda basando la policy su principi di integrità etica

La realizzazione di un efficace modello di organizzazione e gestione ai sensi del D.Lgs. 231/01 richiede diverse competenze integrate: legali, societarie, organizzative e di risk management.

Modello di organizzazione

Un buon modello di organizzazione prevede:

Identificazione dei rischi: dopo un attento esame delle attività e dei processi aziendali si devono identificare le posizioni organizzative assoggettate al rischio reato e le modalità di commissione del reato stesso.

Valutazione dei rischi: i rischi individuati nella prima fase devono essere valutati sulla base della probabilità di accadimento al fine di valutare le eventuali carenze presenti nei controlli esistenti.

Definizione del sistema di controllo: introduzione e coordinamento del sistema dei controlli del rischio reato quali, codice di comportamento, poteri autorizzativi, procedure manuali e informatiche. In questa fase è importante anche la comunicazione a tutti i livelli dell'organizzazione aziendale del sistema di controllo adottato e l'introduzione del sistema disciplinare.

Identificazione di un Organismo di Vigilanza: Individuazione di un organo aziendale che abbia le competenze per poter controllare il processo e definizione esplicita di compiti e responsabilità dell'organo medesimo.

Valutazione e revisione del modello: valutazione periodica dell'efficacia del modello ed esame di eventuali azioni correttive.

Formazione: realizzazione di sessioni formative a tutto il personale anche attraverso piattaforme di e-learning al fine di rendere realmente efficace il modello organizzativo introdotto.

Il modello organizzativo previsto dal D.Lgs. 231/01deve:

-consentire di individuare le attività dell'ente nel cui ambito possono essere commessi reati

-prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente il relazione ai reati da prevenire

-prevedere le modalità di individuazione e gestione delle risorse finanziarie destinate all'attività nel cui ambito possono essere commessi reati

-prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli

-prevedere un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate

Ai sensi del d. lgs. 231/2001, il Modello di organizzazione, gestione e controllo deve essere efficacemente attuato. A tal fine è necessario che sia istituito un apposito Organismo di Vigilanza, incaricato di vigilare in maniera indipendente sul corretto funzionamento e sull'osservanza del Modello.

La composizione dell'Organismo deve essere valutata attentamente a seconda della realtà aziendale e dei rischi individuati, nel rispetto dell'autonomia e dell'indipendenza dello stesso, al fine di consentire a tale organo di svolgere efficacemente i propri compiti.

La normativa riconosce inoltre, in capo a tale organismo, il compito di individuare eventuali aggiornamenti del Modello, anche in funzione delle segnalazioni e indicazioni ricevute da tutti i destinatari del Modello.

Il Codice Etico

Il Codice Etico rappresenta una vera e propria Carta Costituzionale per l'ente e affianca sempre il Modello di organizzazione, gestione e controllo.

E' un documento aziendale volto a individuare diritti, doveri e responsabilità dell'ente e mira a promuovere o vietare alcuni comportamenti che, seppur leciti sotto il profilo normativo, non corrispondano all'etica e ai valori cui l'impresa si ispira nell'esercizio delle proprie attività. Il Codice Etico prevede, inoltre, meccanismi sanzionatori volti ad evitare che passino inosservate le condotte che non rispondono ai valori aziendali e che, pertanto, ne ledono gli interessi.

Analisi per funzioni e per processi

Analisi per funzioni

- L'approccio per funzioni aziendali suggerisce di seguire la suddivisione dei compiti proposta dalla struttura organizzativa, prendendo in esame le attività realizzate all'interno di ciascuna funzione aziendale

Analisi per processi

- L'approccio per processi
  - guida alla creazione del valore per il cliente, in quanto la soddisfazione del cliente ha origine direttamente dai processi e solo indirettamente dalle funzioni;
- consente di identificare più facilmente le responsabilità;
  - spinge a ricercare tutte le attività che non aggiungono valore al prodotto e ad eliminarle.

L’approccio dei processi

Il processo è un insieme di attività intercorrelate, svolte all'interno di un’organizzazione, che creano valore trasformando delle risorse (input del processo) in un prodotto (output del processo) destinato ad un soggetto interno o esterno all’organizzazione (cliente/utente).

Il processo è teso al raggiungimento di un obiettivo.

Il processo è una trasformazione con valore aggiunto.

Ogni processo coinvolge persone e/o risorse. Ogni processo ha input e output.

Un processo è un insieme strutturato di attività,ordinate in modo logico, che utilizzano uno o più input per la realizzazione di un certo risultato.

Ogni processo richiede controlli per assicurare stabilità.

Il documento di valutazione dei rischi

Il Documento di valutazione dei rischi è il frutto di una appropriata analisi dei rischi sui luoghi di lavoro.

La redazione del Documento di valutazione dei Rischi (DVR) deve seguire criteri precisi e deve possedere dei requisiti specifici. In particolare deve contenere una relazione sulla valutazione di tutti i rischi per la sicurezza e la salute durante l'attività lavorativa, nella quale siano specificati i criteri adottati per la valutazione stessa. Una volta individuati i rischi è necessario indicare quali siano le misure di prevenzione e di protezione attuate e i dispositivi di protezione individuali adottati, oltre ad un programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza. Tali misure devono essere giustificate ed è necessario indicare quali siano le procedure da eseguire per la loro attuazione ed i ruoli dell'organizzazione aziendale assegnati unicamente a personale in possesso di adeguate competenze e poteri.

Oltre alle disposizioni per la riduzione dei rischi per la prevenzione e la sicurezza dei lavoratori nei luoghi di lavoro, nel Documento di Valutazione dei Rischi deve essere esplicita l'indicazione del nominativo del Responsabile del Servizio di Prevenzione e Protezione (RSPP), del Rappresentante dei Lavoratori per la Sicurezza (RLS) o di quello territoriale e del Medico Competente. Queste figure devo partecipare alla valutazione dei rischi e alla stesura del DVR insieme al datore di Lavoro (che comunque non può, in nessun caso, esimersi da tale dovere).

In molte realtà lavorative, inoltre, esistono particolari classi di lavoratori esposti a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione e addestramento. All'interno del Documento di Valutazione dei Rischi è necessario individuare in modo univoco tali figure o classi omogenee di lavoratori esposti a particolari rischi.

L'individuazione di rischi specifici richiede la redazione di relazioni inerenti a ognuno di essi. In queste valutazioni dovranno essere riportate le informazioni riguardanti la valutazione dei singoli rischi, la classe dei lavoratori esposti ed i valori di esposizione determinati. Esempi di valutazione di rischi specifici sono:

- Valutazione del Rumore
- Valutazione delle Vibrazioni
- Valutazione delle Radiazioni Ionizzanti
- Valutazione delle Radiazioni Ottiche
- Valutazione delle Polveri e dell'amianto
- Valutazione delle Sostanze Chimiche
- Valutazione delle Sostanze Biologiche

Documento Programmatico sulla sicurezza

Il Documento Programmatico sulla Sicurezza (DPS) o Relazione sul Sistema di Gestione Privacy è un documento interno, che descrive il Modello Privacy Aziendale adottato e nel quale vengono pianificati su base pluriennale gli interventi di adeguamento privacy necessari a rendere conforme il Modello Privacy agli obblighi di legge privacy.

Il DPS (Documento Programmatico sulla Sicurezza) è un documento di pianificazione su base triennale o quinquennale, soggetto ad aggiornamento periodico almeno annuale, composto dalle seguenti sezioni:

- **Introduzione al DPSS**
- **Privacy Policy Aziendale**
- **Organigramma Privacy**
- **Classificazione dei Dati Personali**
- **Classificazione dei Trattamenti**
- **Analisi dei Rischi Privacy**
- **Privacy Gap Analysis**
- **Misure di Sicurezza**
- **Misure Minime di Sicurezza**
- **Trattamenti Affidati all'Esterno**
- **Formazione Privacy**
- **Linee Guida Privacy**
- **Procedure Privacy**
- **Istruzioni Operative Privacy**

L’obbligo formale di redigere o aggiornare il Documento Programmatico sulla Sicurezza (DPS) entro il 31 Marzo di ogni anno, è stato abrogato con il Decreto Legge n. 05/2012 (Decreto Semplificazioni e Sviluppo).

Tuttavia tale modifica normativa non ha eliminato l’obbligo sostanziale di descrivere in una relazione periodica il Sistema di Gestione Privacy adottato.

In particolare il Titolare del Trattamento è ancora gravato dall’onere di formalizzare in un documento programmatico (DPS) l’analisi dei rischi privacy effettuata e le conseguenti misure di sicurezza adottate volte a ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta.

Pertanto, pur essendo venuto meno un obbligo formale di redigere un documento programmatico sulla sicurezza, (DPSS), è rimasto invariato un obbligo sostanziale di descrivere in una relazione periodica privacy, il corretto adempimento delle misure di sicurezza e delle misure minime di sicurezza previste dagli articoli. 34 e 35 del Codice Privacy, così come disciplinate dall’Allegato B del D.lgs. 196/03.

La Relazione sul Sistema di Gestione Privacy coincide, quindi, logicamente e nel contenuto con il Documento Programmatico sulla Sicurezza (DPS), differenziandosi da esso unicamente per il fatto di non dover essere aggiornata obbligatoriamente ogni anno entro una precisa data.

La Relazione sul Sistema di Gestione Privacy è, pertanto, a tutti gli effetti, un documento programmatico sulla sicurezza (DPSS), la cui redazione risulta necessaria e obbligatoria per poter dimostrare, in caso di controlli, alle Autorità Competenti, di avere progettato ed efficacemente attuato un sistema di gestione privacy idoneo a ridurre al minimo tutti rischi privacy che incombono sui dati personali trattati.

La Relazione sul Sistema di Gestione Privacy coincide, quindi, logicamente e nel contenuto con il Documento Programmatico sulla Sicurezza (DPS), differenziandosi da esso unicamente per il fatto di non dover essere aggiornata obbligatoriamente ogni anno entro una precisa data.

La Relazione sul Sistema di Gestione Privacy è, pertanto, a tutti gli effetti, un documento programmatico sulla sicurezza (DPSS), la cui redazione risulta necessaria e obbligatoria per poter dimostrare, in caso di controlli, alle Autorità Competenti, di avere progettato ed efficacemente attuato un sistema di gestione privacy idoneo a ridurre al minimo tutti rischi privacy che incombono sui dati personali trattati.

Le sanzioni previste

L’ente responsabile per un reato commesso da un soggetto appartenente alla sua struttura organizzativa, è condannato da un sistema sanzionatorio che prevede sanzioni amministrative come la sanzione pecuniaria, le sanzioni interdittive , la confisca e la pubblicazione della sentenza di condanna.

Lo scopo delle sanzioni amministrative è quello di colpire direttamente o indirettamente il profitto dell'ente, disincentivando la commissione di reati nell'interesse o a vantaggio dell'ente, e di incidere sulla struttura e sull'organizzazione dell'impresa in modo da favorire attività risarcitorie, Le sanzioni previste per gli illeciti amministrativi dipendenti da reato sono molto severe e si distinguono in:

-sanzioni pecuniarie;

-sanzioni interdittive ;

-confisca;

-pubblicazione della sentenza.

L'art. 10 DLgs. 231/2001 stabilisce che per l'illecito amministrativo dipendente da reato si applica sempre la sanzione pecuniaria e non è ammessa la formula ridotta salvo i casi previsti all'art. 12; la sua determinazione avviene secondo il meccanismo delle quote che si articola in due fasi:

Nella prima fase il giudice fissa l'ammontare del numero delle quote che non deve essere mai inferiore a cento né superiore a mille; ciò avviene grazie alla valutazione della gravità del fatto, del grado di responsabilità dell'ente (adozione di modelli organizzativi, codici etici, sistemi disciplinari), di condotte riparatorie e riorganizzative (sanzioni disciplinari) dopo la commissione del reato.

Nella seconda fase l'organo giurisdizionale determina il valore monetario della singola quota, che va da un minimo di 258 euro ad un massimo di 1549 euro, sulla base delle condizioni economiche e patrimoniali della persona giuridica. Quella pecuniaria e la confisca sono obbligatorie, cioè vengono sempre applicate in caso di condanna.

L'interdizione è quell'istituto giuridico che comporta una limitazione temporanea dell'esercizio di una facoltà o di un diritto, in tutto o in parte; esso è la base delle sanzioni interdittive elaborate dal legislatore per contrastare più efficacemente le condotte illecite all'interno dell'ente grazie al loro contenuto inibitorio.

Le sanzioni interdittive hanno una durata limitata (non inferiore a tre mesi e non superiore a due anni) e possono essere applicate in via definitiva solo secondo quanto stabilito dall'art. 16.

I sistemi di gestione

Sistema di gestione Aziendale	• Pianificazione Aziendale • Budget e controllo di gestione (sistema gestionale rispondente a requisiti normativi in materia contabile e fiscale
Sistema di gestione per la sicurezza sul lavoro	• Dlgs 81/08 e normative in materia di Salute e Sicurezza sul lavoro (OSHAS 18001 – Linee Guida UNI INAIL)
Modello organizzativo ai sensi del Dlgs 231/2001	• DLgs 231/01(sistema gestionale rispondente a requisiti normativi • in materia di responsabilità degli enti per gli illeciti amministrativi dipendenti da reato)
Sistema di gestione ambientale	• T.U. Ambiente - normative in materia di tutela dell'ambiente (UNI EN ISO 14001)

I sistemi di gestione

Sistema di gestione della tutela dei dati Personali e Sensibili	• Dlgs 196/03 (sistema gestionale rispondente a requisiti normativi in materia di tutela dei dati)
Sistema di gestione per la qualità	• UNI EN ISO 9001 (Sistema gestionale volontario • per l'organizzazione che si basa su un approccio per processi)
Sistema di gestione sulla sicurezza ambientale	• HACCP – Analisi dei Rischi e Controllo dei Punti Critici/Pacchetto igiene (DLgs 193/2007 – UNI EN ISO 22000)

Pianificazione aziendale budget e controllo di gestione

Il Sistema di budgeting /controllo di gestione e' un sistema che:

- definisce obiettivi economici da raggiungere
- pianifica costi e ricavi
- tiene sotto controllo i ricavi e soprattutto i costi

e che richiede:

1. una adeguata definizione dell'organigramma, ruoli, funzioni e deleghe
2. la necessità di assegnare budget di spesa specifici ai responsabili di processo a seconda dei centri di costo/ricavo e obiettivo da raggiungere
3. un controllo periodico da parte della direzione
4. la necessità di individuare azioni correttive di spesa

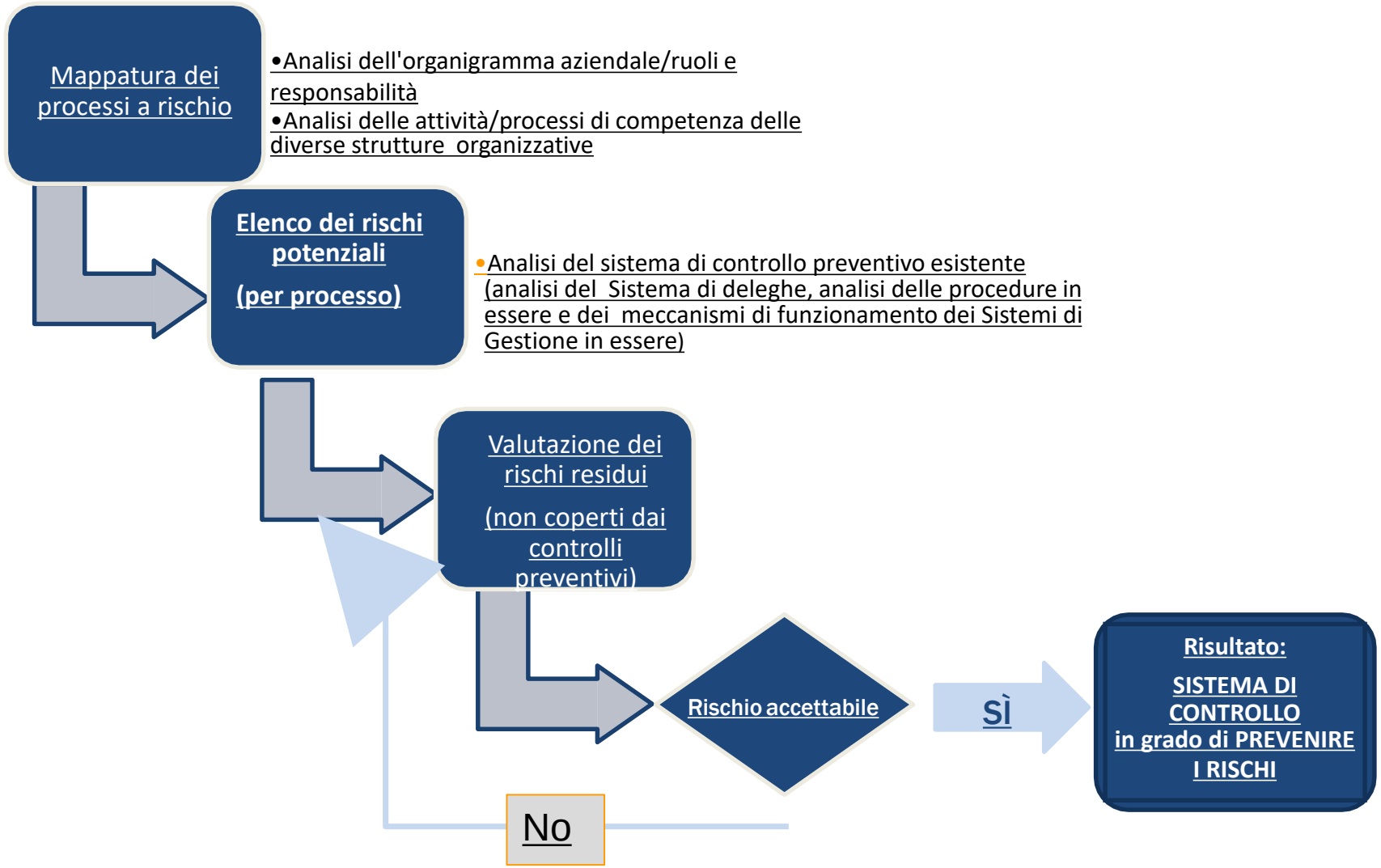
Integrazione dei sistemi

Tutti questi sistemi o modelli approcciano all'organizzazione con un punto di vista molto particolare e specifico che è quello della normativa che li ispira.

Tutti questi modelli a loro volta si orientano all'approccio metodologico ed ai principi del PDCA.

L'integrazione dei sistemi consente di integrare l'approccio organizzativo per processi (es. Analisi dei processi con diagrammi di flusso e definizione di responsabilità) ad una valutazione di efficienza basata anche sull'analisi dei rischi (es. Sicurezza; Haccp; MOG ex 231/01)

Analisi del rischio (le diverse fasi)



La funzione Compliance

Una figura interna che possiede:

- una visione legata all'approccio per processi
- conoscenza dell'organigramma, dei ruoli e delle funzioni aziendali
- conoscenza e capacità di descrivere il funzionamento per processi, che è elemento fondamentale per tutti i sistemi citati e per agevolare l'analisi dei rischi richiesta

È quindi la figura chiave che può favorire un'effettiva interazione fra i sistemi, creando un collegamento tra le diverse figure consulenziali e facendo da riferimento complessivo per la gestione dei sistemi stessi.