ISO 37001
e
Sistemi di Gestione Integrata

Ing. Lucia Venditti

12 luglio 2021

ISO 37001:2016

ISO 37001: **sistema di gestione aziendale anti-corruzione**

Lo standard, certificabile, è stato pubblicato dall'ISO il 15 ottobre 2016

Come tutte le nuove norme rilasciate o quelle da poco revisionate da parte di ISO (ISO 9001:2015, ISO 14001:2015, ISO 45001:2018, ISO 27001:2013), è strutturata secondo la HLS (*High Level Structure*), che ha lo scopo di favorire l'integrazione tra i sistemi di gestione.

È integrabile con gli altri sistemi di gestione.

High Level Structure

Struttura suddivisa in 10 punti principali

•Paragrafi e contenuti che devono essere presenti obbligatoriamente in tutti gli standard

Terminologia, testo, definizioni, titoli e loro sequenza comuni;

•Maggiore importanza al **concetto di rischio.**

•I singoli standard possono aggiungere, ove necessario, requisiti specifici in relazione ai loro campi di applicazione.

Vantaggi

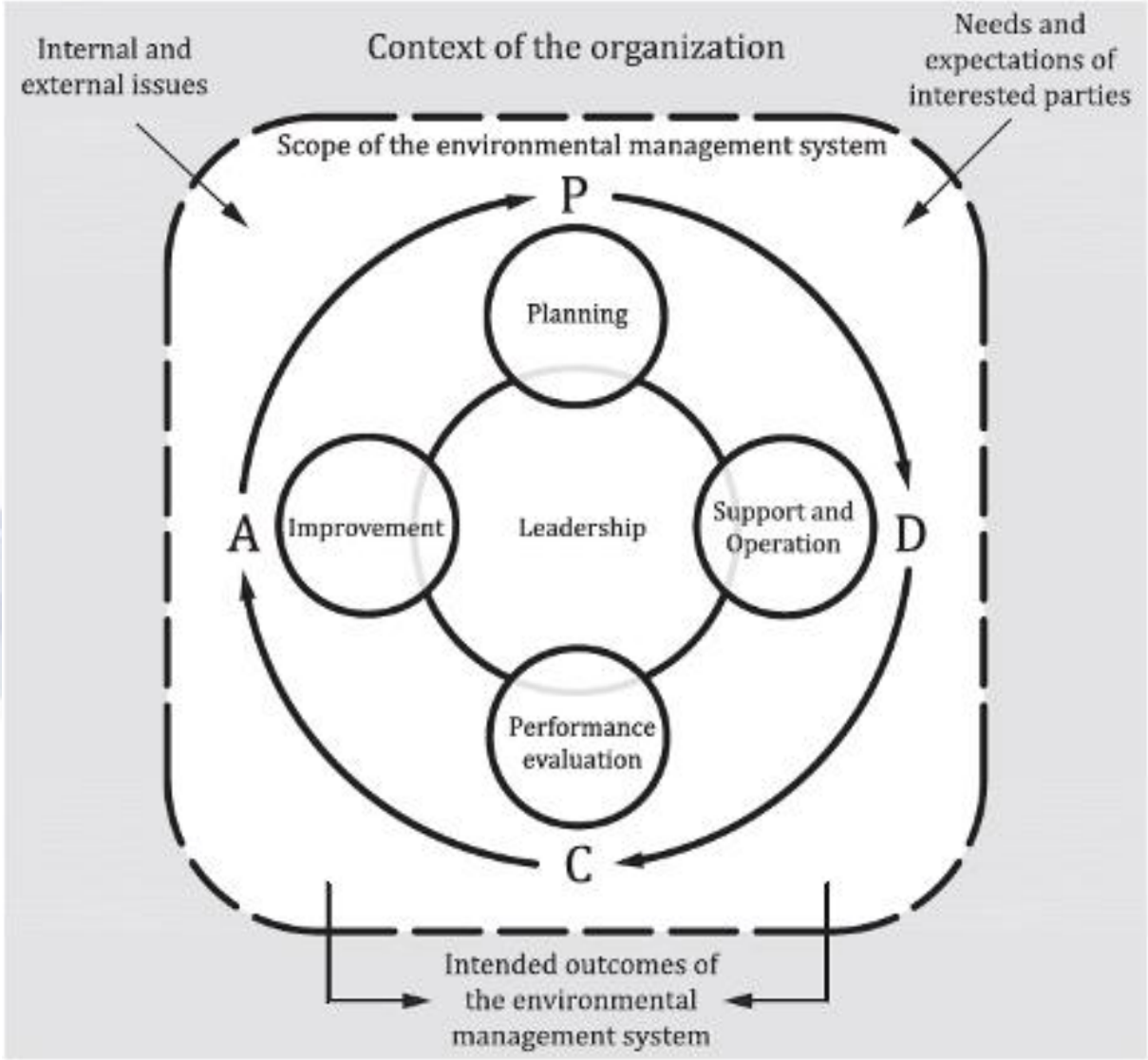
•Maggiore compatibilità con le altre norme;

•Facilità nell'implementare nuovi standard;

•Maggiore facilità nell'integrare le norme in un sistema di gestione;

•Aumentare il valore per gli utenti

PDCA


Internal and external issues
Context of the organization
Needs and expectations of interested parties
Scope of the environmental management system
P
Planning
A
Improvement
Leadership
Support and Operation
D
Performance evaluation
C
Intended outcomes of the environmental management system

Campo d’applicazione

Riguarda tutte le possibili ipotesi di corruzione: non solo la corruzione c.d. pubblica (nei confronti di un pubblico funzionario) ma anche la corruzione tra privati (art 2635 c.c.).

Il suo ambito può essere volontariamente esteso dall’ente ad altri illeciti (ad esempio: riciclaggio, truffa, antitrust)

Mappatura dei rischi

L’ente deve effettuare una mappatura dei rischi di corruzione **(Bribery Risk Assessment)** riferibili alla sua attività.

Tali rischi devono essere valutati in relazione al sistema di controllo interno esistente.

Bribery Risk Assessment

- identificazione e mappatura di tutti i processi a rischio, delle attività correlate a specifiche transazioni, a soci in affari o a personale che possono potenzialmente dar luogo a condotte corruttive;
- redazione di un **organigramma** che illustri chiaramente le responsabilità correlate al processo analizzato, con conseguente individuazione delle deleghe e procure aziendali;
- valutazione dei rischi in riferimento al **contesto esterno ed interno** in cui l'organizzazione opera;
- **esame dei soci in affari/stakeholder** con cui l'organizzazione si relaziona, con annessa valutazione del relativo rischio di corruzione;
- individuazione degli obblighi da rispettare in base a leggi, regolamenti, contratti, adempimenti e doveri professionali

Bribery Risk Assessment

L'organizzazione deve pesare i c.d**. rischi inerenti** (cioè potenzialmente associabili alla sua attività e ai suoi processi), in base alla probabilità di accadimento.

Deve essere misurata l'efficacia preventiva del sistema di controlli esistente.

Se tale ultimo sistema risulterà efficace, contribuirà a mitigare il livello di rischio e a ridurlo ad un livello accettabile (c.d. **rischio residuo**).

Sarà imprescindibile attuare controlli più approfonditi, per processi e soci in affari ad alto rischio e controlli meno impattanti in caso di livello di rischio più basso.

Peraltro, tale **scala di rischio** potrà costituire la base per successive azioni di miglioramento, le quali andranno definite anche con riguardo alla relativa tempistica.

Policy anti-corruzione

Il vertice aziendale deve adottare ed attuare una adeguata **Policy anti-corruzione**.

La Policy deve essere adeguatamente diffusa all'interno dell'ente e ai *business associates*

La Policy deve disciplinare, tra l'altro, il c.d. **whistleblowing**

Funzione di Compliance Anticorruzione

L’ente deve istituire una Funzione di Compliance Anticorruzione **(Anti-bribery Compliance Function).**

Tale Funzione deve supervisionare il sistema; deve fornire pareri sui suoi contenuti e sulla sua applicazione; deve riferire al vertice sui risultati dell’applicazione del sistema.

La Funzione deve avere adeguate **risorse** ed essere **competente** ed **indipendente**.

La Funzione può essere assegnata a soggetti esterni.

Gestione del Personale

L’ente dovrà effettuare **due diligence** in caso di assunzione o trasferimenti e promozioni; in caso di bonus e incentivi (che comunque devono essere ragionevoli).

Il personale interessato dovrà attestare periodicamente il rispetto della Policy anti-corruzione.

Formazione

L’ente dovrà formare il personale, con particolare riguardo alla casistica corruttiva e a come può verificarsi nel suo settore di attività (con riferimento ai c.d. key bribery risk indicators) (**Awareness and training)**

L’ente dovrà coinvolgere nella formazione, se del caso, i *business associates* che svolgono attività per suo conto.

Gestione delle risorse finanziarie

L’ente deve implementare misure di controllo della gestione delle risorse finanziarie, in entrata e in uscita (acquisti, vendite e attività commerciale).

Trattasi di richiesta analoga a quella del d.lgs. 231/2001 relativamente al Modello organizzativo (art 6).

Gifts, hospitality, donations and similar benefits

Donazioni, sponsorizzazioni, liberalità, omaggi e benefit similari vanno regolati nell'ambito della Policy.

Si tratta di erogazioni che possono essere effettuate per fornire utilità diretta o indiretta ad un pubblico funzionario.

Implementation of anti-bribery controls by controlled organizations and by business associates

L’ente deve preoccuparsi anche degli enti controllati, i quali devono, se del caso, adottare la propria policy anti-corruzione.

Raising concerns

L’ente dovrà disciplinare il c.d. whistleblowing, garantendo:

- il riporto della **segnalazione dell’illecito o della violazione del sistema** alla Funzione di Compliance Anti-Corruzione o ad altro soggetto idoneo;
- la **riservatezza** del segnalante e delle parti coinvolte;
- consentendo la segnalazione **anonima**;
- vietando qualsiasi **ritorsione lavorativa** (retaliation) nei confronti del segnalante.

Audit

L’audit è un momento centrale del sistema.

- Gli audits dovranno essere “reasonable, proportionate, and **risk based**”.
- Sono possibili controlli sul *business associate* che non abbia rispettato i contenuti del sistema anti-corruzione.
- L’audit deve essere **imparziale** e può essere svolto dalla Funzione di I.A. oppure dalla Funzione di Compliance Anti-Corruzione o da un auditor esterno.
- L’auditor non può essere legato all’attività sottoposta ad audit.

ISO 37001 e Modello organizzativo 231

Una società che ha adottato un Modello 231 ha interesse ad istituire un SGA ai sensi della ISO 37001 (*SGA aggiuntivo al Modello*)?

Il SG ISO 37001 può rafforzare il Modello 231 relativamente alla prevenzione dei delitti di corruzione (e quindi contribuire positivamente alla valutazione di idoneità ed attuazione del Modello da parte del Giudice penale).

Si pone, cioè, la stessa questione relativa ai rapporti tra Modello 231 e ISO 45001 (già OHSAS 18001) per la sicurezza sul lavoro; tra Modello 231 e la ISO 14001 per i reati ambientali; tra Modello 231 e la ISO 27001 per i reati informatici.

Tuttavia solo in materia di sicurezza sul lavoro c'è un appiglio normativo (art. 30 d.lgs. 81/2008) che valorizza tale rapporto.

ISO 37001 e Modello organizzativo 231

Una società che non ha adottato un Modello 231 potrebbe decidere di istituire un SGA ISO 37001 al suo posto (*SGA alternativo al Modello*)?

In teoria sì ma, così facendo, limiterebbe la possibile copertura dalle sanzioni ex d.lgs. 231 alla sola corruzione (mentre il Modello serve a prevenire numerosi altri reati).

Altri Vantaggi dello standard

Il SGA ISO 37001 può rilevare ai fini del Rating di Legalità

Il regolamento sul Rating prevede alcuni requisiti che, se sussistenti, garantiscono alle imprese il punteggio massimo di 3 stellette. Se ne vengono rispettati almeno 6 si otterranno due stellette.
In particolare le aziende dovranno:
- rispettare i contenuti del Protocollo di legalità sottoscritto dal Ministero dell'Interno e da Confindustria, delle linee guida che ne costituiscono attuazione, del Protocollo sottoscritto dal Ministero dell'Interno e dalla Lega delle Cooperative , e a livello locale dalle Prefetture e dalle associazioni di categoria;
- utilizzare sistemi di tracciabilità dei pagamenti anche per importi inferiori rispetto a quelli fissati dalla legge;
- adottare una struttura organizzativa che effettui il controllo di conformità delle attività aziendali a disposizioni normative applicabili all'impresa o un modello organizzativo ai sensi del d.lgs. 231/2001;
- adottare processi per garantire forme di Corporate Social Responsibility;
- essere iscritte in uno degli elenchi di fornitori, prestatori di servizi ed esecutori di lavori non soggetti a tentativi di infiltrazione mafiosa;
- avere aderito a codici etici di autoregolamentazione adottati dalle associazioni di categoria;
- **aver adottato modelli organizzativi di prevenzione e di contrasto della corruzione.**

GRAZIE!

ing.luciavenditti@gmail.com

Profilo Linkedin