

CONFORMIA

Associazione Organismi Certificazione Ispezione Prove Taratura

CON IL PATROCINIO DI

UNI ENTE ITALIANO
DI NORMAZIONE

n.10
2018

I QUADERNI DI CONFORMIA

**La Linea Guida applicativa
sulla norma UNI ISO 37001:2016
per la prevenzione della corruzione**

©2018 Conforma - Milano

TUTTI I DIRITTI SONO RISERVATI

Nessuna parte del libro può essere riprodotta o diffusa con un mezzo qualsiasi, fotocopie, microfilm, o altro senza il consenso scritto dell'editore.

ALL RIGHTS RESERVED

No part of this work may be reproduced, stored in a retrieval system or transmitted in any form or by any means electronic, photocopying recording or otherwise, without the written permission from the publisher.

Questa pubblicazione non è un documento normativo.
La responsabilità dei concetti espressi è unicamente dell'autore.

Autore

Conforma - Associazione Organismi Certificazione Ispezione Prove Taratura
Piazzale R.Morandi, 2 – 20121 Milano

Editore

Conforma - Associazione Organismi Certificazione Ispezione Prove Taratura
Piazzale R.Morandi, 2 – 20121 Milano

Giugno 2018

La presente Linea Guida nasce come progetto del Gruppo di Lavoro UNI ISO 37001 di Conforma al quale aderiscono i seguenti Soci:

- ASACERT
- AICQ SICEV
- CERTIQUALITY
- DNV GL
- ICIM
- ICMQ
- IMQ
- RINA SERVICES
- SGS

Il documento è il risultato di un tavolo tecnico CONFORMA UNI ISO 37001:2016, al quale hanno partecipato:

Stefano ALDINI	Certiquality	COORDINATORE
Fabrizio CAPACCIOLI	ASACERT	
Federico CARRARO	RINA SERVICES	
Massimo CASSINARI	ICMQ	
Laura CATELLANI	IMQ	
Vincenzo DELACQUA	ICIM	
Laura LIGI	SGS	
Claudio ROSSO	AICQ SICEV	
Valentina SALVI	DNV-GL	

Si ringrazia l'Avv. Mario CASELLATO dello Studio Casellato Avvocati Penalisti di Roma per il prezioso contributo prestato nella revisione delle bozze finali del documento.

Sommario

INTRODUZIONE	7
4 CONTESTO DELL'ORGANIZZAZIONE	9
4.1. Comprendere l'organizzazione e il suo contesto.....	9
4.2. Comprendere le esigenze e le aspettative degli stakeholder.....	11
4.3. Determinare il campo di applicazione del Sistema di Gestione per la prevenzione della corruzione	12
4.4. Sistema di Gestione per la Prevenzione della Corruzione.....	15
4.5. Valutazione del Rischio di Corruzione	16
5 LEADERSHIP	20
5.1 Leadership e impegno.....	20
5.2 Politica per la prevenzione della corruzione.....	22
5.3 Ruoli organizzativi, responsabilità ed autorità.....	23
6 PIANIFICAZIONE	27
6.1 Azioni per affrontare rischi e opportunità	27
6.2 Obiettivi per la prevenzione della corruzione e pianificazione per il loro raggiungimento	28
7 SUPPORTO	29
7.1 Risorse	29
7.2 Competenza	30
7.3 Consapevolezza e formazione	32
7.4 Comunicazione	33
7.5 Informazioni documentate	34
8 ATTIVITÀ OPERATIVE	35
8.1 Pianificazione e controllo operativi	35
8.2 Due Diligence	36
8.3 Controlli finanziari	39
8.4 Controlli non finanziari	41
8.5 Attuazione dei controlli da parte dei soci in affari	44
8.6 Impegni per la prevenzione della corruzione	46
8.7 Regali, ospitalità, donazioni e benefici simili	47
8.8 Gestione dell'inadeguatezza dei controlli per la prevenzione della corruzione	47
8.9 Segnalazione di sospetti	48
8.10 Indagini e gestione della corruzione	49
9 VALUTAZIONE DELLE PRESTAZIONI	50
9.1. Monitoraggio, misurazione, analisi e valutazione	50
9.2. Audit interno	52
9.3. Riesame di direzione	53
9.4. Riesame da parte della funzione di conformità per la prevenzione della corruzione.....	55
10 MIGLIORAMENTO	56
10.1. Non conformità e azione correttiva	56
10.2. Miglioramento continuo	57
ALLEGATO 1 TABELLA DI CORRELAZIONE PTPC / MOG 231 / SISTEMI DI GESTIONE ISO 37001....	58
ALLEGATO 2 TABELLA INTEGRAZIONE REQUISITI ISO 37001 VS ISO 9001:2015.....	60

Introduzione

Linea Guida applicativa sulla UNI ISO 37001:2016

Con la norma UNI ISO 37001, pubblicata a fine 2016, è oggi disponibile su scala internazionale uno standard volontario certificabile che tratta di anti corruzione e che, adottando la medesima struttura comune (cd. "High Level Structure") a tutte le altre norme ISO sui sistemi di gestione delle organizzazioni, rende più agevole la sua integrazione con altri standard largamente diffusi, quali ad esempio la ISO 9001 sui sistemi di gestione per la qualità.

In sintesi, la norma UNI ISO 37001, applicabile a qualsiasi organizzazione pubblica o privata, a prescindere dal settore di attività, dimensioni o localizzazione geografica, stabilisce dei requisiti per pianificare, attuare e mantenere un sistema di gestione e controllo dei rischi di corruzione secondo un approccio che si articola nelle seguenti fasi: analisi e valutazione dei rischi di corruzione, programmazione e attuazione di misure e controlli anti corruzione, sorveglianza sulla loro applicazione e riesame periodico sull'efficacia e adeguatezza del sistema di prevenzione, in modo da assicurarne il miglioramento continuo.

I requisiti della norma volontaria UNI ISO 37001 non rappresentano quindi una novità in senso assoluto in quanto essi riprendono principi, concetti e, in alcuni casi, anche elementi prescrittivi tipici di sistemi e/o modelli di gestione, controllo e prevenzione dei rischi di corruzione previsti da norme di legge in via obbligatoria o con finalità di prova dell'esimente da responsabilità da reato delle organizzazioni (ad esempio, in Italia, i Piani Triennali per la Prevenzione della Corruzione e per la Trasparenza ai sensi della L. 190/2012 e i Modelli di Organizzazione, Gestione e Controllo ai sensi del D.Lgs 231/2001, oppure le misure anticorruzione ai sensi del FCPA statunitense o dell' UK Bribery Act inglese).

Analogamente a quanto previsto per il MOGC ai sensi del D.Lgs 231/2001 per la prevenzione dei reati in materia di salute e sicurezza sul lavoro, con la presunzione di idoneità dei requisiti della norma OHSAS 18001, corrispondenti a quelli di legge (art. 30 del D.Lgs 81/2008), i criteri della norma UNI ISO 37001 possono rappresentare un riferimento valido e autorevole, riconosciuto a livello internazionale, per il modello esimente in ambito corruzione. Inoltre la certificazione di conformità alla norma UNI ISO 37001 da parte di un soggetto terzo indipendente può fornire ulteriori garanzie circa l'adeguatezza e l'effettività del modello ai fini della prova dell'esimente.

Si consideri inoltre che nell'ambito del Piano Nazionale Anticorruzione (PNA) 2016, e in particolare nell'Analisi di Impatto Regolatorio (AIR) che descrive il contesto normativo, le motivazioni e gli obiettivi che hanno portato all'adozione PNA, dando conto delle scelte operate da ANAC con riferimento, in particolare, alle osservazioni più significative formulate in sede di consultazione con riferimento alla metodologia per la gestione del rischio corruzione, si afferma che lo standard UNI ISO 37001 in materia di prevenzione della corruzione consentirebbe di gestire al meglio il rischio corruttivo nelle società e negli enti pubblici.

Proprio in virtù di questi collegamenti tra la norma UNI ISO 37001 e l'applicazione dei sistemi anticorruzione di legge, si è determinato un crescente interesse da parte di ambiti aziendali e professionali, quali ad esempio quello legale, della compliance, dell'internal auditing, che, in molti casi, si sono confrontati occasionalmente o in modo marginale con le norme sui sistemi volontari.

Pertanto, la Linea Guida è rivolta non solo a quanti (auditor, aziende, enti, consulenti, etc) già conoscono le norme ISO e i benefici che possono derivare dalla loro applicazione, se credibile ed effettiva, ma anche a coloro, operatori, esperti e professionisti che potrebbero avere minore dimestichezza con metodologie, tecnicismi e finalità di questi strumenti.

L'obiettivo primario del documento è quello di fornire chiarimenti e indicazioni sull'applicazione dei requisiti della norma UNI ISO 37001 dal punto di vista dell'auditor e sulla base delle esperienze maturate sul campo degli Organismi di certificazione che hanno partecipato alla sua redazione. Con questo approccio più pratico che teorico è evidente che la Linea Guida non ha pretese di esaustività rispetto ai temi trattati, né intende suggerire interpretazioni autentiche dei requisiti della norma UNI ISO 37001.

Tuttavia, si è voluto adottare una chiave di lettura che sottolinei il ruolo della norma UNI ISO 37001 quale criterio omogeneo finalizzato ad ottimizzare il coordinamento e l'integrazione tra i sistemi di controllo dei rischi di corruzione già esistenti nell'organizzazione (PTPC, MOGC 231, procedure ISO 9001, controlli interni, etc.), idoneo a migliorare il monitoraggio sulla loro efficacia e il coinvolgimento dell'intera organizzazione. Ciò significa che l'organizzazione deve partire dai controlli, dalle procedure, dai documenti esistenti e valutare se e in che misura questi siano già idonei a soddisfare i requisiti della UNI ISO 37001 per tenere sotto controllo i rischi di corruzione, evitando quindi inutili, costose e burocratiche duplicazioni di natura meramente formale. D'altronde questo concetto è ben evidenziato dalla stessa norma UNI ISO 37001, che, prima fra tutte le norme ISO, parla di "misure ragionevoli e appropriate", ovvero "appropriate" rispetto al rischio di corruzione e "ragionevoli" in relazione alla probabilità di raggiungere l'obiettivo di prevenire la corruzione.

Con questi presupposti, l'adozione di un sistema di gestione UNI ISO 37001 può costituire un fattore di successo per il controllo dei rischi di corruzione dell'organizzazione, traducendosi in un investimento in legalità e non in un mero costo per l'organizzazione e rappresenta uno degli strumenti per favorire la diffusione di una cultura aziendale contraria alla corruzione, senza la quale nessun sistema di controllo o prevenzione potrà mai dirsi realmente efficace.

Nel testo della Linea Guida viene riportata una sintetica descrizione dei requisiti (colonna a sinistra), con a fronte l'indicazione delle possibili evidenze a supporto della conformità (colonna a destra). Per la descrizione dei requisiti ci si è attenuti a quanto riportato nella testo della UNI ISO 37001:2016 (testo con traduzione italiana) e agli approfondimenti contenuti nella "Guida all'utilizzo" in allegato alla norma. Gli esempi di evidenze riportati in questo documento non sono comunque da considerarsi a nessun titolo esaustivi, ben potendo un'Organizzazione dimostrare la propria conformità altrimenti.

4 CONTESTO DELL'ORGANIZZAZIONE

4.1 Comprendere l'Organizzazione e il suo contesto

Anche la norma UNI ISO 37001, in coerenza con il risk based approach che caratterizza tutte le recenti norme ISO sui sistemi di gestione, richiede preliminarmente all'Organizzazione di determinare i fattori interni ed esterni rilevanti ai fini della pianificazione di un sistema di gestione per la prevenzione della corruzione.

L'identificazione di questi fattori rappresenta un passaggio logico fondamentale ai fini dell'analisi e della valutazione dei rischi di corruzione che possono riguardare l'organizzazione e la programmazione di adeguate misure di riduzione e controllo.

La norma riporta, a titolo di esempio, alcuni di questi fattori, tra cui:

- il modello commerciale dell'organizzazione;
- gli enti sui quali l'organizzazione esercita un controllo e quelli che esercitano un controllo sull'organizzazione;
- i soggetti terzi che operano a vario titolo per conto dell'organizzazione;
- la natura e l'estensione delle relazioni con pubblici ufficiali;
- gli obblighi e gli adempimenti di legge, normativi e contrattuali, rilevanti ai fini della prevenzione della corruzione.

A livello di contesto interno è particolarmente importante per l'organizzazione conoscere e mappare i processi/attività al fine di rilevare quelli "sensibili" a rischio di corruzione. L'approccio per processi (proprio della ISO 9001) viene in questo caso integrato dal concetto di rischio delle norme ISO HLS.

Poiché i fattori interni ed esterni del contesto rappresentano il quadro di riferimento della valutazione dei rischi di corruzione (cfr. p.to 4.5.1), le relative informazioni devono essere mantenute aggiornate. Le eventuali modifiche del contesto sono annoverate tra gli elementi in ingresso del riesame periodico dell'Alta Direzione (cfr. p.to 9.3.1).

L'organizzazione per determinare il campo di applicazione del sistema di gestione per la prevenzione della corruzione deve considerare i fattori interni ed esterni del contesto (cfr. p.to 4.3).

Il requisito non richiede espressamente di dare evidenza documentata dell'analisi del contesto, ma considerato che dette informazioni costituiscono la base conoscitiva per procedere alla valutazione dei rischi e per il suo aggiornamento, è ragionevole attendersi che gli esiti siano documentati per non compromettere l'efficacia e la ripercorribilità del processo di pianificazione del sistema.

Tra gli elementi che l'organizzazione dovrebbe considerare, con particolare attenzione rispetto al proprio contesto interno, vi è quello dell'applicazione di altri sistemi di prevenzione e controllo dei rischi di corruzione previsti da norme di legge che rispondono a principi e criteri analoghi a quelli del sistema UNI ISO 37001 per la prevenzione della corruzione, quali ad esempio:

- i Piani Triennali per la Prevenzione della Corruzione (di seguito indicato anche con l'acronimo PTCP) ai sensi della Legge 190/2012 e smi;
- il Piano Nazionale Anticorruzione (PNA);
- il Modello di Organizzazione, Gestione e Controllo ex D.lgs. 231/2001 (per la parte relativa alla prevenzione dei reati nei rapporti con la Pubblica Amministrazione e per il reato di corruzione tra privati);
- compliance programs ai sensi del Bribery Act inglese o del Foreign Corrupt Practices Act (FCPA) statunitense o di altre normative anticorruzione applicabili all'organizzazione.

Benché questi strumenti abbiano contenuti specifici determinati dalle finalità delle norme di legge che li disciplinano, il loro campo di applicazione si sovrappone a quello del sistema UNI ISO 37001 con il quale condividono i principali elementi: analisi e valutazione del rischio, programmazione e attuazione di misure di controllo commisurate ai rischi, monitoraggio.

Per pianificare il proprio sistema UNI ISO 37001, l'organizzazione dovrebbe considera-

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
	<p>re di integrare a livello organizzativo e operativo i diversi sistemi di prevenzione e controllo dei rischi di corruzione in modo da rispettare sia i requisiti di legge (ad esempio, artt. 6 e 7 del D.lgs. 231/2001 per il Modello Organizzativo o PNA per i PTPC) che quelli del sistema UNI ISO 37001.</p> <p>Questo obiettivo si traduce in una semplificazione perché l'organizzazione può utilizzare gli strumenti a livello organizzativo, gestionale e documentale di cui già dispone per pianificare e attuare un sistema in conformità alla norma UNI ISO 37001, con le opportunità di miglioramento della norma volontaria.</p> <p>L'organizzazione può anche decidere di mantenere sistemi documentali separati, ad esempio, al fine di meglio rispondere alle esigenze di prova del proprio Modello Organizzativo in conformità ai requisiti previsti dal D.lgs. 231/2001. Ma, dove possibile, dovrebbe evitare la duplicazione di strumenti di pianificazione, controllo e monitoraggio che potrebbero determinare inefficienze e disallineamenti a livello organizzativo e gestionale in grado di compromettere la conformità del sistema alla norma UNI ISO 37001 e la prova dell'efficace attuazione del modello di prevenzione nei confronti dei terzi.</p> <p>Per le organizzazioni soggette all'obbligo del Piano Triennale per la Prevenzione della Corruzione ai sensi della Legge 190/2012 e smi, l'analisi del contesto è un requisito espressamente richiamato dal PNA (Piano Nazionale Anticorruzione).</p> <p>Queste organizzazioni dovrebbero già disporre di informazioni documentate all'interno dei PTPC che possono fornire evidenza del rispetto del requisito della norma, sempreché le informazioni risultino complete ed aggiornate in modo da rappresentare in modo congruo e adeguato il contesto dell'organizzazione sotto il profilo della corruzione.</p> <p>In queste situazioni, laddove l'organizzazione abbia stabilito di non integrare l'analisi del contesto prevista per il PTPC con quella della UNI ISO 37001, ma di mantenere documenti</p>

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
	<p>separati, occorre anche valutare la coerenza delle informazioni riportate in tali documenti.</p> <p>Anche l'ottenimento di rating in materia di legalità e trasparenza da parte di autorità pubbliche competenti (in Italia, AGCM - Autorità Garante della Concorrenza e del Mercato) potrebbe rappresentare un elemento da considerare nel contesto interno dell'organizzazione.</p> <p>Ulteriori evidenze circa la comprensione del contesto possono essere raccolte nel corso delle interviste con l'Alta Direzione dell'organizzazione, con il responsabile della compliance per la prevenzione della corruzione, con il Responsabile Prevenzione Corruzione e Trasparenza (RPCT) o membri dell'O.I.V. per le organizzazioni soggette al PTPC, con l'Organismo di Vigilanza (nel caso l'organizzazione abbia stabilito di adottare un Modello di Organizzazione e Gestione ai sensi del D.lgs. 231/2001), con i responsabili di processi a rischio, con rappresentanti di enti sotto il controllo dell'organizzazione.</p> <p>Altre potenziali fonti di informazioni da considerare ai fini dell'analisi del contesto dell'organizzazione sono rappresentate da media a livello locale o nazionale, siti web, osservatori specializzati, etc., che riportano notizie di pubblico dominio e quindi liberamente accessibili circa l'eventuale coinvolgimento dell'organizzazione o di suoi esponenti in fatti o contenziosi rilevanti ai fini dell'applicazione di un sistema di prevenzione della corruzione.</p>
<h4>4.2 Comprendere le esigenze e le aspettative degli stakeholder</h4>	
<p>Parallelamente all'analisi del contesto, la norma richiede all'organizzazione di determinare gli stakeholder rilevanti per il sistema di gestione per la prevenzione della corruzione e di identificare quali siano le esigenze e le aspettative di questi per considerarli nella pianificazione come requisiti che il sistema intende soddisfare.</p> <p>La soddisfazione di questi requisiti incide infatti sulla determinazione dei livelli di rischio e quindi sulla capacità di controllo dei rischi di corruzione dell'or-</p>	<p>Non è richiesto in modo esplicito un elenco documentato delle parti interessate e dei requisiti, aspettative e impegni volontari che li riguardano, rilevanti per il sistema di gestione per la prevenzione della corruzione. Tuttavia, come specificato per il punto precedente, è ragionevole aspettarsi che queste informazioni siano documentate in modo coerente e coordinato con quanto previsto per il processo di valutazione dei rischi, di cui costi-</p>

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
<p>ganizzazione e sugli obiettivi del sistema di prevenzione.</p> <p>Le parti interessate possono essere interne o esterne all'organizzazione (vedi 3.3).</p> <p>La norma UNI ISO 37001 distingue tra requisiti obbligatori di natura cogente, aspettative non obbligatorie degli stakeholder (cui l'organizzazione deve comunque rispondere) e impegni assunti volontariamente verso gli stessi.</p> <p>La pianificazione del sistema UNI ISO 37001 non può infatti prescindere dalla piena consapevolezza circa le prescrizioni di legge o di altra natura in materia di corruzione (derivanti, ad esempio, da protocolli di legalità o da altri accordi con enti, istituzioni, ONG, etc.) riferibili all'organizzazione, così come l'attuazione del sistema non può prescindere dal controllo sulla loro applicazione.</p>	<p>tuiscono uno degli elementi di riferimento. Inoltre, le informazioni sulle esigenze e aspettative degli stakeholders possono rinvenirsi in documenti di cui l'organizzazione già dispone (ad es., bilanci di sostenibilità, PTPC).</p> <p>Analoghe considerazioni valgono per i requisiti cogenti in materia di anti corruzione. Si considerino, ad esempio, gli obblighi sui piani di prevenzione della corruzione, quelli in materia di trasparenza, di conflitto di interessi, di rotazione del personale, in materia di appalti pubblici, etc. Si tratta di un quadro di prescrizioni, requisiti cogenti e raccomandazioni articolato e complesso, soggetto a frequenti modifiche, con fonti di diversa natura (norme di legge, regolamenti, linee guida, etc.). Premesso che la conformità alla norma UNI ISO 37001 presuppone, come per qualsiasi altro standard volontario, il rispetto delle disposizioni di legge in materia di anti corruzione applicabili all'organizzazione in virtù della legislazione dello Stato presso cui viene applicata, occorre valutare se e in che modo l'organizzazione abbia identificato questi requisiti, comprese le modalità per il loro aggiornamento e diffusione presso tutti i responsabili della loro applicazione, e gli strumenti per il monitoraggio sul loro adempimento.</p> <p>La mancanza di informazioni documentate (elenco, registro, etc.) potrebbe pregiudicare la capacità dell'organizzazione di identificare correttamente e di aggiornare tutti gli obblighi in materia di corruzione e la sorveglianza sulla loro applicazione.</p>
<p>4.3 Determinare il campo di applicazione del Sistema di gestione per la prevenzione della corruzione</p>	
<p>La definizione di corruzione cui fa riferimento la norma internazionale ISO 37001 (cfr. p.to 1) è ampia e comprende la corruzione "attiva" (attuata dall'organizzazione, dal personale dell'organizzazione o anche, indirettamente, tramite soggetti terzi) e quella "passiva" (compiuta nei confronti dell'organizzazione o del suo personale) e si estende a considerare anche la corruzione (sia attiva che passiva) dei cd. "soci in affari", terze parti con cui l'orga-</p>	<p>La verifica circa la corretta determinazione del campo di applicazione del sistema UNI ISO 37001 rappresenta un passaggio logico preliminare di fondamentale importanza per la valutazione della conformità alla norma. Occorre quindi verificare se i processi/attività, nonché le sedi e i siti presso i quali vengono svolti tali processi/attività, identificati nel campo di applicazione, sia-</p>

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
<p>nizzazione ha relazioni commerciali (cfr. p.to 8.5). Con riferimento a questi ultimi, si precisa che il termine “business associates” della edizione internazionale ISO della norma è stato tradotto nella versione UNI con “soci in affari” e che questo termine verrà quindi utilizzato nella presente Linea Guida, in aderenza alla traduzione italiana ufficiale.</p> <p>Questa definizione deve essere riesaminata alla luce del significato di “corruzione” ai sensi della legislazione dello Stato presso il quale lo standard viene applicato dall’organizzazione. E’ importante ricordare che una norma volontaria, quale la UNI ISO 37001, presuppone sempre l’obbligo di conformarsi agli obblighi di legge applicabili, rispetto ai quali il sistema di gestione rappresenta uno strumento finalizzato a migliorare il controllo dei rischi di corruzione dell’organizzazione.</p> <p>Una volta chiarito il significato di corruzione cui fare riferimento, l’organizzazione deve determinare il campo di applicazione del sistema di gestione per la prevenzione della corruzione, stabilendo così il perimetro entro il quale sono applicati i requisiti della norma.</p> <p>Il campo di applicazione deve essere documentato e deve essere disponibile alla parti interessate se l’organizzazione dichiara di essere conforme allo standard.</p> <p>Per determinare il campo di applicazione l’organizzazione deve tenere in considerazione gli elementi previsti dal requisito della norma:</p> <ul style="list-style-type: none"> - i fattori interni ed esterno del contesto, individuati ai sensi del paragrafo 4.1; - i requisiti riconducibili alle parti interessate e in particolare gli obblighi di legge in materia di anti corruzione; - gli esiti della valutazione dei rischi di corruzione di cui al successivo paragrafo 4.5. <p>Nella definizione di “outsourcing” si chiarisce che un’organizzazione esterna non fa parte del sistema UNI ISO 37001, anche se a questa siano stati affidati processi che rientrano nel campo di applicazione del sistema dell’organizzazione.</p> <p>La “guida sull’utilizzo della norma” (Allegato A) fornisce alcune indicazioni relative ai pagamenti cd “agevolativi” ed “estorti” allo scopo di chiarire, se e in che misura, siffatti comportamenti debbano o meno rientrare nel campo di applicazione del sistema UNI ISO 37001.</p> <p>Con riferimento al pagamento “agevolativo” di</p>	<p>no coperti dal sistema UNI ISO 37001. Se la valutazione è finalizzata al rilascio di una certificazione accreditata, occorre tenere conto delle regole del sistema di accreditamento in merito al campo di applicazione (in Italia, la circolare tecnica Accredia n. 28/2017 - Informativa in merito all’accreditamento per lo schema di certificazione UNI ISO 37001 – Prevenzione della corruzione).</p> <p>In considerazione delle aspettative delle parti interessate rispetto al sistema per la prevenzione della corruzione, appare comunque problematico ammettere la possibilità di escludere processi ed attività a rischio non basso di corruzione dal campo di applicazione. Tale possibilità poi sarebbe certamente esclusa quando l’adozione di un sistema di prevenzione del rischio di corruzione da parte dell’organizzazione è oggetto di uno specifico obbligo di legge (ad es. i Piani per la prevenzione della corruzione ai sensi della Legge 190/2012).</p> <p>Occorre poi valutare se l’organizzazione abbia indentificato puntualmente la definizione di “corruzione” cui fa riferimento il proprio sistema UNI ISO 37001, tenuto conto che il significato di “corruzione” è stabilito dalla legislazione in materia, vigente nello Stato (o negli Stati) presso cui è applicato lo standard. In Italia, i principali riferimenti per la fattispecie penale sono costituiti dall’art. 318 del Codice Penale (Corruzione per l’esercizio della funzione), dall’art. 319 del Codice Penale (Corruzione per un atto contrario ai doveri d’ufficio) e dall’art. 2635 del Codice Civile (Corruzione tra privati).</p> <p>Per le organizzazioni soggette agli adempimenti della Legge 190/2012, l’identificazione del rischio non deve limitarsi a considerare soltanto i comportamenti illeciti ma anche quelle condotte che, pur non avendo rilevanza penale, determinano un malfunzionamento dell’ amministrazione a causa dell’uso a fini privati delle funzioni pubbliche (c.d maladministration).</p> <p>Infine occorre valutare la coerenza del campo di applicazione con il contesto interno ed esterno in cui opera l’organizzazione e con i requisiti delle parti interessate, inclusi gli</p>

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
<p>somme, di norma di bassa entità, corrisposte per ottenere o velocizzare interventi di “routine” comunque dovuti da parte di un “funzionario” pubblico, la norma UNI ISO 37001 sottolinea come tali pagamenti, da considerarsi come “tangenti” a tutti gli effetti, dovrebbero essere vietati dal sistema di gestione per la prevenzione della corruzione.</p> <p>I pagamenti “estorti” in quanto ottenuti sotto minacce alla propria incolumità o libertà fisica e/o psicologica non rientrano nel campo di applicazione della norma UNI ISO 37001.</p> <p>Si raccomanda tuttavia all’organizzazione di fornire istruzioni al proprio personale su come affrontare richieste di pagamenti “agevolativi” od estorti e su come comportarsi nel caso si sia proceduto a tali pagamenti, prevedendo azioni appropriate (indagini sull’accaduto, registrazioni dei pagamenti, segnalazioni alla autorità competenti).</p> <p>Nella “Guida all’utilizzo” della ISO 37001 (vedi A.3) si afferma espressamente un principio comune a tutti i sistemi volontari, di primaria importanza ai fini della loro efficace attuazione. Le misure di controllo dei rischi di corruzione debbono essere ragionevoli ed appropriate. Ciò significa che le misure non possono essere così esose, onerose e burocratiche da renderle insostenibili o tali da bloccare le attività dell’organizzazione, o talmente semplici e inefficaci da consentire facilmente la corruzione.</p> <p>Si tratta di un principio che deve guidare l’organizzazione nella progettazione e attuazione del proprio sistema di prevenzione della corruzione e che diventa anche un possibile criterio di cui tenere conto nella valutazione della conformità alla norma. Misure di controllo inappropriate (rispetto all’organizzazione) o irragionevoli (rispetto agli obiettivi che si prefiggono), anche se formalmente corrette, potrebbero infatti compromettere la conformità del sistema di gestione per la prevenzione della corruzione.</p>	<p>obblighi di legge in materia di anti corruzione. Questo significa che l’organizzazione per pianificare, stabilire e attuare il sistema di gestione UNI ISO 37001, dovrebbe aver considerato, tra l’altro:</p> <ul style="list-style-type: none"> - la sussistenza di altri sistemi o regole per la prevenzione dei rischi di corruzione cui è tenuta per legge (ad es. piani prevenzione corruzione ai sensi della Legge 190/2012; compliance programs ai sensi del FCPA statunitense) o che abbia stabilito di adottare per non incorrere in responsabilità e sanzioni a carico dell’ente/società (ad es., Modelli Organizzativi ai sensi del D.lgs. 231/2001; procedure adeguate ai sensi del Bribery Act inglese); - la presenza di organizzazioni di cui detiene il controllo, secondo le definizioni stabilite dalla legislazione in materia; - i “livelli di influenza” sui soci in affari che, operando per conto dell’organizzazione, determinano rischi di corruzione rilevanti (ad esempio, società o enti che detengono il controllo dell’organizzazione; partner in consorzi, associazioni temporanee di imprese, etc); - i sistemi di controllo dei rischi di corruzione che tali soci in affari applicano (o potrebbero applicare) nei rapporti con l’organizzazione; - le operazioni di acquisizione, in essere o programmate, di altre organizzazioni o di parte di esse; - l’attuazione di un sistema di gestione della qualità conforme alla norma ISO 9001:2015, in forza del quale l’organizzazione potrebbe già applicare procedure e presidi integrabili con il sistema di prevenzione della corruzione (ad esempio, procurement, audit interni, non conformità e azioni correttive, riesame dell’Alta Direzione). <p>I processi con rischi di corruzione superiori al livello basso che siano stati affidati all’esterno (ad es., a un’altra società del gruppo di appartenenza dell’organizzazione) devono essere compresi nel campo di applicazione del sistema UNI ISO 37001. La capacità di controllo di questi rischi da parte dell’orga-</p>

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
	<p>nizzazione viene valutata nell'ambito dei requisiti relativi ai soci in affari, di cui possono fare parte "i fornitori" (cfr. p.to. 3.17 della norma).</p>
<p>4.4 Sistema di Gestione per la Prevenzione della Corruzione</p>	
<p>Secondo la norma UNI ISO 37001 (cfr. p.to. 3.55 della norma), il sistema di gestione è l'insieme di elementi dell'organizzazione (quali ruoli e responsabilità, strumenti di programmazione, processi, procedure), che sono tra loro correlati o che interagiscono per realizzare obiettivi di prevenzione della corruzione.</p> <p>La definizione è importante per sottolineare come il sistema di gestione costituisca parte integrante dell'organizzazione e che i suoi requisiti governano i processi aziendali e le loro interazioni in modo da raggiungere gli obiettivi di prevenzione della corruzione, nell'ottica del miglioramento continuo comune alle altre norme volontarie ISO.</p> <p>Adottare un sistema di gestione significa pertanto individuare e attuare strumenti e risorse aziendali, che, organizzati e applicati secondo i requisiti della norma, concorrono al raggiungimento di questi obiettivi. Il sistema UNI ISO 37001 non può risolversi in una struttura "sulla carta" che si sovrappone in modo artificioso e incoerente rispetto alle modalità di funzionamento dell'organizzazione, ma deve piuttosto farne parte integrante, espressione di un finalità di prevenzione della corruzione di cui tenere conto (per quanto pertinente) in ogni fase o aspetto dell'attività aziendale.</p> <p>L'approccio basato sul rischio è il criterio guida per progettare, stabilire e attuare il sistema UNI ISO 37001.</p> <p>Questo richiede in sintesi il requisito in oggetto, da considerarsi una sorta di "chiave di lettura" non solo per le organizzazioni che attuano un sistema UNI ISO 37001 ma anche per tutti coloro che devono valutarne la conformità alla norma.</p>	<p>Questo requisito, di importanza fondamentale, ma di natura generale e "programmatica" rispetto allo sviluppo del sistema, pone alcune difficoltà sotto il profilo della valutazione della conformità e, in particolare, delle evidenze da raccogliere a supporto di tale giudizio.</p> <p>Il primo aspetto da considerare riguarda l'integrazione del sistema di gestione per la prevenzione nei processi dell'organizzazione e quindi nella documentazione aziendale (ad es. organigrammi, programmazioni pluriennali, piani operativi, piani di controllo e sorveglianza).</p> <p>In Italia, per le organizzazioni della Pubblica Amministrazione, l'integrazione del sistema di prevenzione della corruzione di legge (PTPC) nel "piano delle performance" dell'Ente è oggetto di specifica prescrizione.</p> <p>Nell'ambito di questo requisito va inoltre valutata l'organizzazione complessiva aziendale per il controllo dei rischi di corruzione in presenza di altri strumenti (ad es., modelli organizzativi ai sensi del D.lgs. 231/2001) che perseguono le medesime finalità del sistema UNI ISO 37001.</p> <p>Pur non essendo obbligatoria per la UNI ISO 37001 la "formale" integrazione dei diversi sistemi di prevenzione della corruzione applicati dall'organizzazione, quest'ultima deve comunque averli considerati nel campo di applicazione e deve dimostrare che la scelta organizzativa adottata è in grado di assicurare un efficace livello di controllo di questi rischi e la conformità agli obblighi di legge applicabili.</p> <p>L'auditor dovrebbe inoltre verificare e valutare mediante interviste al top management, ai titolari di deleghe e ai responsabili dei processi con rischi di corruzione superiori al livello</p>

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
	<p>basso, la capacità dell'organizzazione di:</p> <ul style="list-style-type: none"> - assicurare l'attuazione della policy anti corruzione nelle strategie aziendali; - incorporare il sistema di gestione della prevenzione della corruzione nel sistema aziendale mediante l'attribuzione di responsabilità adeguate e un idoneo controllo dei processi; - garantire flussi efficaci di comunicazione e risposte adeguate; - identificare, analizzare e valutare i rischi di corruzione in modo coerente con le attività e il contesto dell'organizzazione; - revisionare il sistema di controllo e prevenzione dei rischi in conseguenza di potenziali o effettivi cambiamenti.
4.5.Valutazione del Rischio di Corruzione	
<p>Per la norma UNI ISO 37001, come per le altre norme ISO sui sistemi di gestione, l'analisi e la valutazione dei rischi rappresenta l'elemento alla base della progettazione, dell'attuazione e del mantenimento del sistema di gestione per la prevenzione della corruzione.</p> <p>Nella logica della prevenzione, una corretta e puntuale identificazione e valutazione dei rischi di corruzione assicura la programmazione e l'attuazione di misure adeguate ed efficaci a contrastare questi rischi.</p> <p>Questo significa che laddove la rilevazione dei rischi sia carente o insufficiente, o la valutazione di questi rischi sia incompleta o inadeguata, il sistema di controllo e l'attuazione delle misure di cui è costituito non saranno in grado di raggiungere risultati efficaci di prevenzione.</p> <p>Il rischio, secondo le norme ISO che adottano la cd. "High Level Structure" (HLS), è infatti definito come un effetto dell'incertezza sul raggiungimento dei risultati attesi ed assume una connotazione di "neutralità" che può avere un'accezione sia negativa sia positiva (definita come "opportunità").</p> <p>La corruzione rappresenta uno dei fattori (al pari di quelli trattati dalle altre norme volontarie, ISO 9001, ISO 14001, ISO 45001) che può influire sull'attuazione delle strategie dell'organizzazione e sul raggiungimento dei suoi obiettivi, in primis in termini di compliance e di gestione etica del business.</p>	<p>Come detto, per pianificare e realizzare un solido sistema di gestione della prevenzione della corruzione, è di fondamentale importanza assicurare una corretta "Gestione del Rischio", opportunamente integrata con gli adempimenti normativi cogenti applicabili, in funzione della tipologia di organizzazione.</p> <p>La verifica del processo di gestione del rischio di corruzione dovrebbe partire dalla rilevazione e dalla mappatura dei processi (o sub-processi o attività) dell'organizzazione che sono potenzialmente a rischio di corruzione ("rischi ragionevolmente prevedibili"). Quale che sia la metodologia prescelta dall'organizzazione, occorre quindi valutare se essa abbia consentito di:</p> <ul style="list-style-type: none"> - mappare correttamente e adeguatamente tutti i processi "a rischio" in relazione alla natura, all'attività, al contesto dell'organizzazione etc.; - di identificare i processi sensibili in modo sufficientemente analitico e dettagliato per rappresentare i rischi di corruzione ad essi connessi (ad es., la rilevazione di un processo in termini eccessivamente generici, senza dare conto delle sue diverse fasi, ben difficilmente condurrà ad una corretta identificazione e valutazione dei rischi specifici ed a pianificare un efficace sistema di controllo).

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
<p>Il requisito della norma UNI ISO 37001 non prevede una specifica metodologia per la valutazione e il trattamento dei rischi di corruzione, ma definisce i passaggi fondamentali che l'organizzazione deve mettere in atto per pianificare e attuare il sistema di prevenzione (cd "risk based approach").</p> <p>La metodologia e i criteri da applicare per identificare e ponderare i rischi sono rimessi alla discrezionalità dell'organizzazione in funzione della sua natura, tipo di processi, complessità, settore di attività, etc. (cfr. A.4.1 della "Guida all'utilizzo", ove si richiama, "per ulteriori istruzioni" non obbligatorie, la Linea Guida ISO 31001).</p> <p>Laddove vi siano disposizioni di legge o requisiti di altro tipo (ad es. indicazioni delle autorità competenti in materia di corruzione) applicabili, l'organizzazione deve considerare tali prescrizioni per stabilire metodologie e criteri di valutazione dei rischi di corruzione.</p> <p>La valutazione del rischio corruzione parte dall'analisi degli elementi esterni ed interni del contesto dell'organizzazione, compresi i requisiti degli stakeholder, rilevanti ai fini del raggiungimento degli obiettivi fissati dal sistema di gestione per la prevenzione della corruzione (cfr. p.to 4.1).</p> <p>Sulla base delle informazioni relative al proprio contesto, secondo la norma UNI ISO 37001, l'organizzazione deve:</p> <ul style="list-style-type: none"> - identificare i rischi di corruzione che "possa ragionevolmente" prevedere; - analizzare e ponderare i rischi di corruzione identificati in modo da assegnare loro una scala di priorità; - valutare idoneità ed efficacia del sistema dei controlli esistenti a contenere i rischi stimati. <p>Come detto in precedenza, l'organizzazione deve altresì definire i criteri per dimensionare i livelli di rischio di corruzione.</p> <p>La norma richiede che l'analisi dei rischi sia documentata e comprensiva delle informazioni relative alla correlazione tra gli esiti della valutazione dei rischi e la programmazione delle misure di controllo.</p> <p>Coerentemente con quanto previsto dalle norme ISO, il risk assessment è un processo dinamico e non statico.</p> <p>Pertanto la norma pone particolare enfasi nella valutazione periodica del rischio corruzione presente nell'organizzazione e indica la necessità di un perio-</p>	<p>Come evidenziato in precedenza, è a discrezione dell'organizzazione, in funzione delle proprie caratteristiche e della tipologia operativa, definire le modalità con cui viene effettuata la valutazione del rischio di corruzione, la metodologia applicata, il modo di ponderare e dare priorità ai rischi di corruzione e il livello accettato o tollerato di rischio corruttivo.</p> <p>In ogni caso, occorre valutare se l'organizzazione abbia considerato eventuali obblighi o indicazioni di legge relativi alla metodologia da seguire per la valutazione dei rischi (ad esempio, quelli relativi all'attuazione dei Piani di Prevenzione della Corruzione e della Trasparenza ai sensi della Legge 190/2012 e del PNA) con l'obiettivo di armonizzarli con quanto previsto dal sistema di gestione UNI ISO 37001, anche al fine di evitare inutili e ridondanti duplicazioni di attività.</p> <p>Se l'organizzazione abbia stabilito di adottare procedure e controlli dei rischi di corruzione onde evitare od attenuare eventuali responsabilità (ad esempio, il Modello Organizzativo previsto dal D. Lgs 231/2001; procedure e controlli ai sensi del Bribery Act), il sistema di gestione UNI ISO 37001 fornisce dei criteri applicativi aggiuntivi per la valutazione dei rischi di corruzione rispetto a quelli di legge. La norma UNI ISO 37001 richiede che questi criteri, oggettivi e ripercorribili, conducano a dei risultati in grado di rappresentare la situazione dei rischi di corruzione dell'organizzazione in modo adeguato e continuativo, anche rispetto a eventuali cambiamenti o modifiche. Sotto tale profilo si coglie la natura "dinamica" del processo di gestione del rischio UNI ISO 37001, il quale richiede un riesame della valutazione da pianificare e aggiornare ad intervalli regolari.</p> <p>Ciò premesso, indipendentemente dalla metodologia prescelta dall'organizzazione, occorre verificare se siano stati definiti in modo esplicito criteri idonei a rappresentare e valutare i rischi, in modo coerente con il contesto, con la "politica" e con gli obiettivi di prevenzione della corruzione.</p> <p>Ad esempio, questi criteri potrebbero fare rife-</p>

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
<p>dico riesame, sotteso a rilevare nuove informazioni e/o cambiamenti significativi dell'organizzazione, con l'obbligo di conservazione della documentazione atta a comprovare l'avvenuta valutazione del rischio.</p>	<p>rimento alla natura pubblica o privata dell'organizzazione e dei soci in affari, a quello del settore di attività (ad esempio, se percepito a elevato rischio di corruzione), alla dimensione organizzativa, sino a definire indici interni di corruzione, ai fini di agevolare il processo di valutazione.</p> <p>Ulteriori fattori da considerare potrebbero, a mero titolo di esempio, riguardare:</p> <ul style="list-style-type: none"> - i processi/attività tipici dell'organizzazione, che in modo endemico possono essere maggiormente soggetti ad atti corruttivi, quali, ad esempio, accordi compensativi e/o accordi che coinvolgono i soci in affari, soprattutto quando questi ultimi potrebbero configurare un conflitto di interessi; - il modello commerciale prescelto dall'organizzazione, con particolare riferimento all'operato di agenti e/o intermediari che interagiscono direttamente con clienti, ed in generale a qualunque rapporto commerciale basato su margini provvigionali; - l'analisi dei ricavi desunti da operazioni con marginalità nettamente superiori alla media (fronte clienti) o da forniture di valore particolarmente rilevanti (fronte fornitori); - il recente coinvolgimento in indagini giudiziarie o contenziosi per fatti di corruzione o illeciti analoghi; - la dislocazione dell'organizzazione in paesi percepiti ad elevato rischio corruttivo (cfr. CPI – Corruption Perception Index realizzato da Transparency International). <p>Infine, occorre considerare i casi in cui vi siano requisiti cogenti o di altro tipo che stabiliscono il rischio di corruzione o la metodologia di un processo/attività.</p> <p>E' il caso delle organizzazioni soggette alla normativa per la prevenzione della corruzione (Legge 190/2012 e PNA) per le quali sono state predefinite "Aree di Rischio Generali", comuni a tutte, cui ciascuna organizzazione dovrà aggiungere le "Aree di Rischio Specifiche", tipiche della propria attività (per la cui valutazione si applicheranno i requisiti della norma UNI ISO 37001).</p> <p>Uguualmente, dovrebbero essere tenute in considerazione le metodologie proposte dalle Linee Guida emesse dalle associazioni di</p>

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
	<p>categoria di riferimento per le organizzazioni che hanno deciso di adottare un Modello Organizzativo ai sensi del D.lgs. 231/2001 (ad esempio le “Linee Guida 231 di Confindustria”).</p> <p>Occorre poi verificare se l’organizzazione, mediante l’applicazione dei criteri prescelti, abbia dato un ordine di priorità ai rischi valutati in funzione del peso loro attribuito. Questa informazione è importante per l’organizzazione al fine di orientare e supportare la pianificazione delle azioni e le relative decisioni.</p> <p>Pur non potendo entrare nel merito specifico della metodologia scelta dall’organizzazione, occorre valutare se il risultato della valutazione del rischio possa considerarsi coerente con la natura e le caratteristiche della stessa, con i processi e le attività, con il contesto. E’ possibile effettuare questa verifica ripercorrendo, ad esempio, l’applicazione dei criteri seguita dall’organizzazione per più processi/attività, campionati in funzione dei relativi livelli di rischio, con il diretto coinvolgimento del responsabile di quei processi/attività.</p> <p>Occorre poi verificare se nell’analisi dei rischi l’organizzazione abbia preso in considerazione i controlli esistenti a presidio del rischio, non in linea astratta, ma valutandone l’efficacia e l’idoneità sotto il profilo operativo, come richiesto dal p.to 4.5.3.</p> <p>L’organizzazione deve pertanto fornire evidenza di aver determinato il tipo e il livello di controllo per la prevenzione della corruzione associato a ogni categoria di rischio individuato ed esprimere un giudizio sull’adeguatezza del controllo in essere a contenere il rischio. Il livello di rischio viene quindi determinato dalla combinazione tra rischio del processo/attività ed efficacia dei controlli atti a contenere il rischio.</p> <p>Nel caso in cui i controlli potrebbero essere migliorati contribuendo a diminuire i livelli di rischio, l’organizzazione pianificherà le azioni necessarie, come stabilito dal successivo p.to 6.1.</p>

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
	<p>Infine, occorre verificare se le procedure dell'organizzazione prevedano l'effettuazione di un riesame della valutazione dei rischi, a cadenze regolari, in modo da valutare in modo complessivo l'impatto dei cambiamenti intervenuti nell'intervallo di tempo considerato e la capacità di assorbire tale impatto, aggiornando (ove necessario) i livelli di rischio e predisponendo le misure necessarie, in funzione delle mutate situazioni organizzative ed operative dell'organizzazione.</p> <p>In ogni caso, occorre verificare se l'organizzazione abbia tempestivamente reagito ai cambiamenti significativi, coinvolgendo i responsabili coinvolti, ridefinendo i livelli di rischio e aggiornando tempestivamente le misure di controllo per contenere eventuali effetti negativi. A tale riguardo l'organizzazione potrebbe stabilire delle procedure (o integrare quelle esistenti) per la gestione dei cambiamenti e delle modifiche che tengano conto di eventuali impatti anche sotto il profilo dei rischi di corruzione (cfr. p.to 8.2 in tema di due diligence).</p> <p>Poiché il riesame riguarda anche l'adeguatezza del processo di controllo, l'organizzazione potrebbe fornire evidenza di un piano di sorveglianza, che preveda, con riferimento a ciascun processo a rischio da verificare (cosa), i controlli da applicare (come), la frequenza (quando) e le responsabilità (chi).</p>
5 LEADERSHIP	
5.1 Leadership e impegno	
5.1.1 Organo Direttivo	
<p>L'introduzione del riferimento all' "Organo Direttivo", e la conseguente distinzione dall' "Alta Direzione" ("Top Management") rappresentano una novità nel panorama delle norme ISO.</p> <p>In base alla UNI ISO 37001 (cfr. p.to 3.7), l'Organo Direttivo è definito come un "gruppo o un organo":</p> <ul style="list-style-type: none"> - che sotto il profilo "funzionale", detiene le responsabilità ultime e l'autorità sull'amministrazione, sulla governance e sulle politiche dell'organizzazione, ivi compresa quella per la prevenzione della 	<p>Le evidenze a supporto della valutazione di conformità al requisito possono riguardare:</p> <ul style="list-style-type: none"> - iter di approvazione della politica per la prevenzione della corruzione (verbali di riunioni, documento di politica con firma in calce del presidente del CdA o del Comitato in calce alla politica, etc.); - verbali di riunione dell'Organo Direttivo con il riesame del sistema di gestione (cfr. p.to 9.3.2) comprensivo delle informazioni trasmesse dall'Alta Direzione e dalla funzio-

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
<p>corruzione di cui il sistema di gestione UNI ISO 37001 costituisce attuazione;</p> <ul style="list-style-type: none"> - cui riporta e risponde l'Alta Direzione dell'organizzazione. <p>Esempi di "Organo Direttivo" possono essere (a titolo non esaustivo) il Consiglio di Amministrazione, i comitati del Consiglio di Amministrazione, il Consiglio di sorveglianza, (nel sistema di governance c.d. "dualistico"). L'individuazione dell'Organo Direttivo dipende comunque dal sistema di governance dell'organizzazione.</p> <p>L'applicazione di questo requisito è ovviamente esclusa in tutti i casi in cui non sia presente un Organo Direttivo come per le organizzazioni di piccole dimensioni.</p> <p>La norma UNI ISO 37001 richiede che l'Organo Direttivo:</p> <ul style="list-style-type: none"> - approvi e confermi la politica in materia di prevenzione della corruzione; - stabilisca strategie coerenti con queste politiche; - riesami a intervalli programmati le informazioni relative al sistema di gestione per la prevenzione della corruzione che gli vengono riferite dall'Alta Direzione e dalla funzione di conformità per la prevenzione della corruzione; - eserciti una sorveglianza ragionevole (commisurata cioè alle proprie funzioni e prerogative) sull'attuazione del sistema di gestione, richiedendo lo stanziamento di risorse adeguate affinché questo funzioni in modo efficace. <p>Queste attività devono essere svolte dall'Alta Direzione allorché non sia presente l'Organo Direttivo. Nelle pubbliche amministrazioni l'Organo Direttivo può essere identificato con gli organi di governo che esercitano le funzioni di indirizzo politico-amministrativo, definendo gli obiettivi ed i programmi da attuare e verificando la rispondenza dei risultati dell'attività amministrativa e della gestione agli indirizzi impartiti.</p>	<p>ne di conformità per la prevenzione della corruzione concernenti il contenuto e il funzionamento del sistema di gestione, relazioni dall'Alta Direzione;</p> <ul style="list-style-type: none"> - informazioni documentate relative alla pianificazione strategica dell'organizzazione; - verbali di riunione dai quali si evinca l'applicazione di tutti i requisiti del paragrafo 5.1.1.
5.1.2 Alta Direzione	
<p>La norma identifica il concetto di Alta Direzione come: "persona o gruppo di persone che, al livello più elevato, dirigono e controllano un'organizzazione" (cfr. p.to 3.6).</p> <p>L'Alta Direzione ha la responsabilità di attuare e mantenere il sistema di gestione per la prevenzione della corruzione, con approccio orientato al mi-</p>	<p>L'effettiva leadership ed impegno dell'Alta Direzione nei riguardi del sistema di gestione è uno dei requisiti più difficili da valutare sulla base di evidenze oggettive e circostanziate. Molti elementi possono essere rilevati in modo trasversale in diversi requisiti della norma nel corso di tutto l'audit. Singolarmente</p>

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
<p>grioramento continuo, impiegando risorse adeguate per il suo funzionamento.</p> <p>A tale fine, e fatto salvo quanto detto con riferimento all'Organo Direttivo (se presente), all'Alta Direzione è richiesto di dimostrare il proprio ruolo di guida e coinvolgimento nel sistema di gestione per la prevenzione della corruzione:</p> <ul style="list-style-type: none"> - assicurando l'integrazione del sistema di gestione nei processi dell'organizzazione; - sostenendo le funzioni preposte a prevenire e individuare la corruzione nelle loro aree di competenza ad acquisire consapevolezza circa il loro ruolo; - comunicando all'interno e all'esterno la politica di prevenzione della corruzione dell'organizzazione; - promuovendo la cultura della lotta alla corruzione all'interno dell'organizzazione, con il contributo di tutto il personale, proponendosi come guida e ausilio a tale scopo; - incoraggiando l'uso di procedure di segnalazione di atti di corruzione certi o presunti; - assicurandosi che nessun membro del personale subisca ritorsioni o minacce o conseguenze disciplinari per il fatto di aver effettuato tali segnalazioni o per essersi rifiutato di prendere parte ad atti di corruzione, anche nel caso in cui questo possa comportare un danno al business dell'organizzazione. 	<p>considerati essi rappresentano dei "segnali" in grado di fondare un giudizio complessivo sull'effettiva volontà da parte dell'Alta Direzione di mettere a disposizione del sistema di gestione le risorse necessarie, di pretendere l'applicazione della politica e delle regole del sistema da parte di tutta l'organizzazione (e in primis da parte della stessa Alta direzione), di integrare il sistema di gestione nei processi dell'organizzazione.</p> <p>Elementi utili per la verifica di quanto sopra possono essere (a titolo di esempio):</p> <ul style="list-style-type: none"> - intervista con l'Alta Direzione per valutarne la consapevolezza e l'effettivo impegno con riferimento alla politica, agli obiettivi, ai rischi di corruzione dell'organizzazione; - sistema delle deleghe (cfr. p.to 5.3.3); - ruoli e responsabilità per la prevenzione e il controllo dei rischi di corruzione (cfr. p.to 5.3.1); - verbale del riesame di direzione (cfr. p.to 9.3.1); - obiettivi per la prevenzione della corruzione e integrazione di questi obiettivi nelle strategie e negli strumenti di programmazione dell'organizzazione (cfr. p.to 6.2); - interviste al personale, verifica dell'effettivo coinvolgimento; - integrazione con altri sistemi di prevenzione e controllo della corruzione; - verifica dell'efficacia delle azioni correttive sotto il profilo delle risorse messe a disposizione; - gestione delle segnalazioni di casi di corruzione presunti o reali (cfr. p.to 8.9); - relazioni all'Organo Direttivo.
5.2 Politica per la prevenzione della corruzione	
<p>La politica di prevenzione della corruzione è emessa a cura dell'Alta direzione dell'organizzazione ed approvata dall'Organo Direttivo, se presente. Essa esprime in modo formale l'impegno alla prevenzione della corruzione, fornendo il quadro di riferimento per il sistema di gestione.</p> <p>La politica deve essere disponibile in forma documentata e divulgata internamente all'organizzazione, ai soci in affari considerati non irrilevanti per</p>	<p>La politica di prevenzione della corruzione non può essere avulsa dal sistema di gestione. Oltre agli elementi di carattere formale che devono essere espressamente riportati nel documento (impegno alla conformità alle leggi in materia di corruzione, impegno a soddisfare i requisiti del sistema e al miglioramento continuo, incoraggiamento a utilizzare gli strumenti di segnalazione degli atti di corruzione, indipendenza e autorità della funzione</p>

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
<p>rischi corruttivi, oltre ad essere resa disponibile alle parti terze.</p> <p>La politica deve inoltre illustrare le conseguenze derivanti da non conformità alla stessa.</p>	<p>di conformità per la prevenzione della corruzione, conseguenze delle non conformità alla politica), occorre verificare che la politica sia coerente con:</p> <ul style="list-style-type: none"> - le caratteristiche, le dimensioni dell'organizzazione e il campo di applicazione del sistema di gestione; - l'analisi del contesto; - le aspettative delle parti interessate; - la valutazione dei rischi; - gli obiettivi identificati; <p>È necessario inoltre valutare le evidenze della comunicazione della politica all'interno dell'organizzazione e ai soci in affari con rischi superiori al livello basso, valutando nel corso delle interviste al personale se essa sia conosciuta e compresa.</p>

5.3 Ruoli organizzativi, responsabilità ed autorità

5.3.1 Ruoli e responsabilità

<p>Il punto 5.3.1 della norma disciplina ruoli e responsabilità all'interno dell'organizzazione, precisando che l'Alta Direzione deve avere la complessiva responsabilità in merito all'attuazione ed osservanza del sistema di prevenzione della corruzione (cfr. p.to 5.1.2).</p> <p>Il requisito definisce due ulteriori livelli di responsabilità, oltre a quello "apicale", sulla complessiva attuazione del sistema.</p> <p>All'Alta Direzione è richiesto infatti di definire, assegnare e comunicare le responsabilità e l'autorità nell'ambito del processi e delle attività svolte, ad ogni livello dell'organizzazione.</p> <p>Manager (e owners di processi/attività) ad ogni livello sono pertanto responsabili della corretta applicazione e dell'osservanza dei requisiti richiesti dal sistema di gestione per le funzioni, aree e reparti di loro competenza.</p> <p>Tutti i membri del personale (a partire dall'Organo Direttivo, se presente, e dall'Alta Direzione) rispondono dell'applicazione e dell'osservanza dei requisiti del sistema di gestione per la prevenzione che afferiscono al loro ruolo nell'organizzazione.</p>	<p>Dovrebbero essere disponibili organigrammi, disposizioni organizzative, mansionari.</p> <p>Tuttavia, a seconda della complessità delle organizzazioni, delle attività e dei rischi di corruzione associati, può essere considerata accettabile una definizione delle responsabilità a livello di:</p> <ul style="list-style-type: none"> - flusso dei processi; - procedure gestionali; - istruzioni operative; - accessi riservati ai sistemi informativi aziendali. <p>E' sempre opportuno accertarsi dell'effettiva rilevanza nell'organizzazione dei ruoli cui siano state assegnate responsabilità e autorità e della coerenza tra quanto formalmente risulta in base ad organigrammi, mansionari, etc. e quanto riscontrato di fatto nel corso dell'audit su funzioni, aree, processi ed attività in cui sono stati rilevati rischi di corruzione.</p> <p>Con riferimento a quanto sopra, occorre verificare se la persona (o le persone) assegnata alla funzione compliance per la prevenzione della corruzione, siano munite dello status, dell'autorità e dell'indipendenza richiesti dal ruolo, oltre che delle competenze necessarie (cfr. p.to 5.3.2).</p>
---	---

5.3.2 Funzione di conformità per la prevenzione della corruzione

Il punto norma prevede che sia l'Alta Direzione ad assegnare a una funzione di conformità per la prevenzione della corruzione, le responsabilità e l'autorità per supervisionare la progettazione, fornire consulenza e guida al personale circa il sistema implementato, assicurare che il sistema sia conforme ai requisiti e relazionare sulla prestazione del sistema stesso all'Organo Direttivo (se presente) e gli altri organi/funzioni nel modo più opportuno.

Nello specifico l'ampiezza e la struttura della funzione dipenderanno dalla dimensione dell'azienda, dall'attività svolta e dalla tipologia di processi sensibili svolti.

In ogni caso, alla funzione di conformità per la prevenzione della corruzione deve essere attribuita la facoltà di riportare direttamente all'Organo Direttivo (se presente) o all'Alta Direzione le criticità relative ad atti di corruzione o a violazioni del sistema di gestione.

Per le organizzazioni di piccole dimensioni, parte o tutte le funzioni di conformità per la prevenzione della corruzione possono essere affidate a soggetti esterni all'organizzazione.

In tal caso, l'Alta Direzione deve assicurare che questi soggetti esterni assumano le responsabilità e dispongano di autorità adeguate all'incarico, comunicandole all'interno dell'organizzazione.

La valutazione degli elementi che consentono di determinare il grado di competenza, status, autorità ed indipendenza della funzione può avvenire attraverso:

- verifica degli atti di nomina;
- verifica del riesame della direzione;
- verifica delle procedure operative specifiche per la corretta operatività della funzione;
- interviste al personale per verificare la consapevolezza dello stesso in merito alla funzione;
- verifica di verbali di formazione, attestati, esperienze e qualifiche professionali;
- verifica dell'effettiva operatività della funzione compliance in termini di risorse (umane, finanziarie, organizzative etc.);
- verifica dei verbali di riunione della funzione e di comunicazione tra questa e l'Alta Direzione / all'Organo Direttivo (se presente).

Laddove i compiti della funzione siano stati affidati a soggetti esterni all'organizzazione, gli aspetti sopra indicati, e in particolare l'autorità, la continuità d'azione e la capacità di intervento su questioni afferenti l'anti corruzione, devono essere considerati con particolare attenzione.

Particolarmente critica è l'indipendenza della funzione anticorruzione che verrà verificata attraverso controlli su organigramma operativo, istruzioni operative e mansionario, al fine di verificare l'assenza, per quanto possibile, di sovrapposizioni tra la funzione anticorruzione e attività esposte a rischio corruttivo.

A tal fine potrà essere utile verificare anche la presenza di budget adeguati all'espletamento della funzione, atti a garantire sufficiente autonomia.

Nel caso di affidamento della funzione (o parti di esse) a soggetti esterni (soci in affari) occorre verificare l'adeguatezza dell'oggetto dell'incarico in contratto rispetto a quanto richiesto dal requisito, ed effettuare interviste al personale al fine di valutare l'effettiva continuità d'azione della funzione e la sua autorità all'interno dell'organizzazione.

Inoltre, va ricordata l'eventualità che un

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
	<p>membro dell'Organismo di Vigilanza ai sensi del D.lgs. 231/2001 (ove presente) possa ricoprire il ruolo di funzione anticorruzione o far parte di essa, sempre che ciò risulti compatibile con i requisiti di indipendenza e autonomia richiesti ai componenti dell'Organismo di Vigilanza (OdV) in presenza di mansioni operative che potrebbero inficiarne l'obiettività di giudizio.</p> <p>Limitatamente a quanto di pertinenza del sistema di gestione UNI ISO 37001, questi aspetti potrebbero essere valutati, a mero titolo di esempio, mediante un approfondimento circa:</p> <ul style="list-style-type: none"> - la separazione dei ruoli e delle funzioni ove possa delinarsi un conflitto d'interesse (ad es. prevedendo una turnazione dei membri dell'OdV o astensione dello stesso dalle attività di audit di vigilanza); - la garanzia di un budget specifico per l'attività di prevenzione anticorruzione diverso da quello stabilito per l'OdV; - la presenza di strumenti idonei per garantire l'assenza di conflitti d'interesse; - l'accesso diretto e tempestivo all'Organo Direttivo e all'Alta Direzione. <p>Infine, è opportuno sottolineare il parallelismo tra la funzione di conformità del sistema UNI ISO 37001 e il Responsabile della Prevenzione Corruzione e della Trasparenza (RPCT) ai sensi della Legge 190/2012.</p> <p>Nel caso di organizzazioni soggette all'obbligo di nominare il RPCT, è necessario che queste considerino di integrare, o quanto meno di coordinare, sotto il profilo organizzativo e funzionale la figura del RPCT con quella della funzione di conformità per la prevenzione della corruzione.</p> <p>A tale riguardo, occorre ricordare che in base alle Linee Guida ANAC sulle Società partecipate, ad oggi:</p> <ul style="list-style-type: none"> - le funzioni di RPCT devono essere affidate a un dirigente della società; - solo in circostanze eccezionali (non chiarite da ANAC) l'amministratore della società può coincidere con il RPCT, purché sia privo di deleghe gestionali; - nel caso in cui la società sia priva di dirigenti, o, nel caso di organizzazioni di ridotte dimensioni questi siano in numero così li-

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
	<p>mitato da non poter essere distolti da attività gestionali su aree a rischio corruttivo, le funzioni di RPCT possono essere assegnate a non dirigenti, a condizione che siano muniti delle necessarie competenze e che il CdA (o l'AU) eserciti una vigilanza intensa e periodica sul loro operato.</p> <p>In tale ultimo caso, l'attuazione di un sistema di gestione per la prevenzione della corruzione in conformità alla norma UNI ISO 37001 rappresenta lo strumento mediante il quale il vertice della Società potrebbe agevolmente dimostrare la vigilanza esercitata sull'attività del RPCT (non dirigente).</p> <p>Le Linee Guida ANAC sconsigliano anche che il RPCT possa far parte dell'OdV ai sensi del D.Lgs 231/2001.</p> <p>Sotto il profilo delle responsabilità (di tipo dirigenziale, disciplinare, per danno erariale e all'immagine della pubblica amministrazione) che incombono sul RPCT in caso di commissione di un reato di corruzione, accertato con sentenza passata in giudicato, è opportuno anche ricordare come l'attuazione di un sistema di gestione UNI ISO 37001 (ancor più ove certificato) potrebbe supportare la prova da parte dello stesso RPCT dell'esimente di avere proposto un PTPCT con misure adeguate e di aver vigilato sul funzionamento e sull'osservanza dello stesso.</p>
5.3.3 Deleghe nel processo decisionale	
<p>Anche questa rappresenta una novità rispetto alle altre norme ISO in quanto vengono stabiliti, ai fini della conformità alla norma UNI ISO 37001, i requisiti del processo di delega per il contenimento dei rischi di corruzione.</p> <p>Il focus della norma riguarda infatti attività/processi che presentano rischi di corruzione superiori al livello basso, rispetto ai quali l'Alta Direzione abbia deciso di delegare a soggetti terzi l'autorità di prendere (in tutto o in parte) decisioni che spetterebbero ad essa. Con il trasferimento dell'autorità di prendere decisioni si determinano anche le conseguenti responsabilità in capo al delegato, che si aggiungono a quelle dell'Alta Direzione (o dell'Organo Direttivo, se presente).</p> <p>La norma non entra nel merito dell'efficacia libera-</p>	<p>Nella verifica del processo di delega verranno verificate le procedure specifiche per la delega includendo un'analisi di quanto segue:</p> <ul style="list-style-type: none"> - procedure organizzative; - formalizzazione degli atti di delega in coerenza con le disposizioni di legge applicabili; - indicazione delle soglie di approvazione delle spese effettuate dal delegato; - specificazione delle competenze richieste e dei poteri conferiti al delegato; - accettazione dell'incarico; - coerenza dei poteri autorizzativi e di firma con le responsabilità assegnate; - due diligence finalizzata a investigare eventuali profili di conflitto di interesse soggetti-

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
<p>toria e dell'opponibilità ai terzi della delega le quali dipendono dai requisiti di legge applicabili caso per caso. Tali requisiti devono essere comunque presi in considerazione dall'organizzazione per stabilire il proprio sistema della deleghe.</p> <p>Due sono invece le condizioni dettate dalla norma UNI ISO 37001.</p> <p>La prima di natura generale, riguarda l'attribuzione al delegato di poteri (e risorse) adeguati per decidere e attuare le proprie decisioni "con autorità" rispetto a quanto oggetto di delega. Diversamente, il trasferimento ad altri soggetti del potere di prendere decisioni in seno all'organizzazione risulterebbe meramente fittizio.</p> <p>In secondo luogo, tra i requisiti di "idoneità" che il delegato deve possedere e mantenere nel tempo vi è quello dell'assenza di conflitti di interesse (attuali o potenziali) rispetto alle decisioni che viene chiamato a prendere all'interno dell'organizzazione.</p> <p>Pertanto, se l'Alta Direzione abbia deciso di delegare l'autorità di assumere decisioni in relazione a cui sussista un rischio di corruzione superiore al livello basso, devono esserci una procedura o dei controlli a presidio di queste condizioni.</p> <p>Come detto, in caso di delega l'Alta Direzione non può disinteressarsi delle proprie responsabilità per l'osservanza e l'attuazione del sistema per la prevenzione della corruzione; pertanto la norma UNI ISO 37001 richiede all'Alta Direzione di sottoporre a verifica periodica i processi di delega.</p>	<p>vi (persona del delegato) o rispetto a quanto oggetto di delega;</p> <ul style="list-style-type: none"> - procedure operative specifiche. <p>Le metodologie di controllo e valutazione periodica devono garantire l'idoneità dei processi decisionali e dei livelli di autorità per i quali sia stata attribuita delega, definendo altresì una periodicità dei controlli, per valutare e risolvere nel tempo le intervenute ipotesi di conflittualità reali e potenziali.</p> <p>Verrà inoltre verificata la corretta mappatura delle deleghe/poteri per verificare l'assenza di duplicazione di ruoli, garantendo quindi una corretta distribuzione delle funzioni all'interno dell'organizzazione.</p> <p>Quest'ultimo aspetto ha particolare rilevanza nel caso in cui l'azienda si sia dotata di un modello organizzativo ex D.lgs. 231/2001. In questo caso è necessaria una corretta mappatura di deleghe e controlli già in essere al fine di evitare una duplicazione delle attività, garantendo in ogni caso l'efficacia del sistema di gestione. Di conseguenza potrebbero essere valutati positivamente quei controlli specifici effettuati in fase di assessment/aggiornamento del Modello relativi alla mappatura dei poteri e deleghe assegnate.</p>
<h2>6 PIANIFICAZIONE</h2>	
<h3>6.1 Azioni per affrontare rischi e opportunità</h3>	
<p>Gli output del processo di analisi e valutazione dei rischi, nell'ambito del quale sono ricompresi anche i fattori del contesto (cfr. p.to 4.5.1), forniscono il quadro di riferimento per pianificare azioni di trattamento e controllo dei rischi di corruzione dell'organizzazione.</p> <p>Anche la capacità dell'organizzazione di rispondere ai requisiti che riguardano le parti interessate e, soprattutto, di ottemperare agli obblighi di legge in materia di prevenzione della corruzione, rappresentano fattori critici che devono essere considerati nella pianificazione del sistema.</p> <p>Secondo la logica della norma volontaria UNI ISO 37001, a differenza dei modelli di prevenzione e</p>	<p>Poiché il requisito sulla pianificazione riguarda il trattamento dei rischi identificati e valutati secondo quanto previsto dal p.to 4.5.1, la verifica di conformità dovrebbe essere effettuata nell'ambito del processo di gestione dei rischi dell'organizzazione.</p> <p>In particolare, occorre verificare:</p> <ul style="list-style-type: none"> - la correlazione e la coerenza tra i risultati della valutazione dei rischi di corruzione e le azioni e i presidi programmati e/o stabiliti dall'organizzazione; - per ciascuna azione pianificata e attuata, i controlli stabiliti per sorvegliarne l'applica-

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
<p>controllo dei rischi previsti ex lege, questo non è l'unico obiettivo che deve perseguire il sistema di gestione per la prevenzione della corruzione. L'organizzazione infatti deve pianificare (e attuare) interventi che assicurino anche il miglioramento continuo del proprio sistema di gestione. In pratica, all'organizzazione è richiesto non solo di tenere sotto controllo i propri rischi, ma di migliorare i livelli di controllo e prevenzione di questi rischi, compatibilmente con le risorse a disposizione (umane, organizzative, economiche, finanziarie, etc.), definendo obiettivi appropriati secondo quanto richiesto dal successivo vedi 6.2.</p> <p>L'organizzazione deve monitorare l'efficacia del sistema e delle azioni intraprese per contenere i rischi e per migliorare i livelli di controllo di questi rischi stabilendo, laddove fattibile, opportuni indicatori (cfr. p.to 9).</p> <p>Queste informazioni rappresentano i principali elementi da portare all'esame dell'Alta Direzione (e dell'Organo Direttivo, se presente) al fine di apportare eventuali interventi correttivi (cfr. p.to 9.3), assicurando così il miglioramento continuo del sistema di gestione per la prevenzione della corruzione (cfr. p.to 10).</p> <p>Oltre ai rischi, l'organizzazione deve considerare nella fase di pianificazione anche le "opportunità" di miglioramento che potrebbero derivare dall'attuazione di efficaci interventi di controllo e mitigazione dei rischi di corruzione.</p>	<p>zione, con le relative responsabilità;</p> <ul style="list-style-type: none"> - l'andamento dei livelli di rischio rilevati dall'organizzazione in relazione all'attuazione delle misure di controllo e di miglioramento: eventuali peggioramenti dei livelli di rischio denotano scarsa efficacia delle azioni intraprese che dovrebbero essere portate all'immediata attenzione dell'Alta Direzione dell'organizzazione; - identificazione delle opportunità di miglioramento (ove presenti) derivanti dalla pianificazione del sistema riguardanti, ad esempio i rapporti con le parti terze interessate (ed, in primis, le autorità competenti in materia di corruzione), l'immagine e la reputazione aziendale sul mercato, la previsione di eventuali criteri premiali per l'affidamento di appalti pubblici o per l'acquisizione di commesse etc.
6.2 Obiettivi per la prevenzione della corruzione e pianificazione per il loro raggiungimento	
<p>La definizione di obiettivi chiari, raggiungibili e misurabili è uno degli elementi fondamentali per monitorare e migliorare l'efficacia del sistema di gestione. Gli obiettivi devono prevedere azioni ed interventi ("cosa sarà fatto") idonei a conseguire i "risultati" attesi nell'ambito del sistema di gestione per la prevenzione della corruzione e ai fini del miglioramento dei livelli di rischio.</p> <p>Affinché questi obiettivi non restino mere dichiarazioni di intenti occorre che siano stabiliti, in modo documentato, tempi, risorse, responsabilità per il loro conseguimento e le conseguenze derivanti dalla mancata attuazione.</p> <p>Condizione necessaria è, ovviamente, che gli obiettivi siano comunicati a tutto il personale coinvolto nel loro raggiungimento e rivisti periodicamente.</p>	<p>La verifica di conformità al requisito dovrebbe avvenire attraverso l'esame degli obiettivi definiti dall'organizzazione e della loro coerenza con i risultati dell'analisi del rischio di corruzione: è ragionevole ritenere che, per le situazioni che l'analisi dei rischi di corruzione identifica come "critiche" o comunque di rischio elevato, siano definiti obiettivi di miglioramento.</p> <p>Viceversa, qualora si riscontrasse che l'organizzazione ha deciso di dedicare risorse significative per situazioni che l'analisi dei rischi di corruzione non ha preso in considerazione o ha identificato come rischio basso è legittimo porsi dei dubbi sull'efficacia del processo di</p>

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
<p>Possibili esempi di obiettivi potrebbero comprendere:</p> <ul style="list-style-type: none"> - adozione di un software gestionale per migliorare il monitoraggio aziendale su ciclo attivo e passivo; - integrazione della procedura relativa agli approvigionamenti prevedendo (entro limiti ragionevoli e in funzione dei rischi) la richiesta di almeno tre preventivi; - riduzione degli importi al sopra dei quali è necessario un doppio livello di autorizzazione per le richieste di finanziamenti; - incremento della quota prevista per la rotazione del personale che ricopre ruoli critici per quanto riguarda l'esposizione alla corruzione; - adozione di una piattaforma per la gestione del whistleblowing. <p>Si tratta di esempi puramente indicativi che ogni organizzazione deve individuare e definire in funzione delle proprie caratteristiche, della valutazione dei rischi e della propria politica per la prevenzione della corruzione.</p> <p>In particolare, occorre stabilire e monitorare quali siano i risultati derivanti dall'attuazione dell'obiettivo in termini di contenimento e miglioramento dei livelli di rischio di corruzione.</p>	<p>analisi dei rischi e/o di definizione degli obiettivi.</p> <p>Occorre valutare la modalità di comunicazione degli obiettivi al personale attraverso l'esame di documenti (comunicazioni, ordini di servizio ecc...) ma anche e soprattutto attraverso colloqui con il personale stesso.</p> <p>In particolare andrebbe intervistato il responsabile dell'obiettivo che di norma (ma non necessariamente) coincide con il responsabile del processo/attività a rischio cui l'obiettivo e le relative azioni si riferiscono.</p> <p>Occorre valutare la documentazione che comprovi, per ciascun obiettivo, la predisposizione da parte dell'organizzazione di una adeguata pianificazione (tempistiche, responsabilità, risorse, metodi di valutazione dei raggiungimento del risultato) e le ricadute sulla valutazione dei rischi che derivano dal conseguimento dell'obiettivo, in relazione ai risultati attesi.</p>
7 SUPPORTO	
7.1 Risorse	
<p>L'Organizzazione deve definire e fornire le risorse (umane, organizzative, finanziarie) e gli strumenti (ad es, software gestionali) necessari a consentire l'attuazione, il mantenimento e il miglioramento nel tempo del sistema di gestione per la prevenzione della corruzione.</p> <p>L'efficacia del sistema dipende infatti dalle risorse messe a disposizione, attraverso le quali si manifesta anche l'effettivo impegno dell'Alta Direzione a raggiungere gli obiettivi aziendali per il contrasto e la prevenzione della corruzione.</p>	<p>Elementi utili a valutare la conformità a questo requisito possono essere raccolti in modo trasversale nel corso dell'interviste.</p> <p>L'evidenza di uno scarso coinvolgimento del personale dell'organizzazione, e in particolare delle funzioni maggiormente a rischio di corruzione, potrebbe rappresentare il segnale di una carenza strutturale di risorse, e, a cascata, quello di un basso livello di coinvolgimento di coloro che hanno l'autorità per assegnarle. Questi segnali, pur non rappresentando delle evidenze in senso stretto, dovrebbero indurre l'auditor ad approfondire i processi decisionali dell'organizzazione, in relazione, ad esempio, agli strumenti di programmazione e di rendicontazione economica e gestionale, agli organigrammi, alle anomalie e alle carenze riscontrate dai controlli, allo stato di conformità rispetto ad obblighi cogenti che riguardano la prevenzione della corruzione. L'obiettivo è di</p>

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
	<p>comprendere, attraverso elementi concreti e ripercorribili, se le risorse messe a disposizione sono adeguate rispetto agli obiettivi del sistema di gestione per la prevenzione della corruzione.</p>
7.2 Competenza	
7.2.2 Processo di assunzione	
<p>I requisiti sul processo di assunzione rappresentano una novità rispetto alle altre norme ISO. Si tratta infatti di un processo identificato a rischio significativo di corruzione, rispetto al quale l'organizzazione deve predisporre una serie di misure riguardanti tutto il personale (cfr. p.to 7.2.2.1) e, in particolare, coloro che occupano, o sono destinati ad occupare, posizioni organizzative con rischi di corruzione superiori al livello basso (cfr. p.to 7.2.2.2).</p> <p>L'organizzazione deve prevedere condizioni di assunzione che includano l'impegno a rispettare la politica e il sistema di gestione per la prevenzione della corruzione e consentano di punire eventuali violazioni, attivando misure disciplinari adeguate e conformi alla legge e ai contratti.</p> <p>L'organizzazione deve quindi fornire, o rendere comunque accessibile, ai neo assunti la politica per la prevenzione della corruzione, assicurando che questi siano formati sul suo contenuto.</p> <p>Inoltre l'organizzazione deve assicurare che tutti i membri del personale non subiscano ritorsioni o minacce per essersi rifiutati di prendere parte a collaborare ad attività rispetto alle quali abbiano ragionevolmente valutato la presenza di rischi di corruzione superiori al livello basso, ovvero per aver segnalato, "in buona fede e sulla base di una convinzione ragionevole", di atti di corruzione (tentati, effettivi o anche presunti) o di violazioni della politica e del sistema di gestione per la prevenzione della corruzione.</p> <p>Prima dell'assunzione (o di un cambio mansioni), la norma UNI ISO 37001 richiede che sia effettuata una due diligence sui membri del personale cui sia assegnata una posizione organizzativa con livelli di rischio superiori al basso (ad es. il responsabile degli acquisti, quello dell'ufficio gare, il responsabile del contenzioso o quello del controllo interno, il responsabile delle risorse umane, etc.). Tra questi</p>	<p>Questi requisiti, pur collocati nella norma tra quelli relativi alla "competenza" e alla formazione del personale, prevedono a tutti gli effetti "controlli" e misure per prevenire i rischi di corruzione correlati al processo di selezione e assunzione del personale dell'organizzazione (cfr. p.to 8).</p> <p>La valutazione di conformità a questi requisiti potrà essere effettuata mediante:</p> <ul style="list-style-type: none"> - l'avvenuta consegna di copia della politica al momento dell'assunzione o comunque la messa a disposizione a tutto il personale dell'organizzazione mediante adeguati strumenti; - l'analisi della documentazione contrattuale e delle lettere di assunzione del personale per verificare la presenza degli impegni al rispetto della politica e del sistema di prevenzione della corruzione; - l'analisi dell'applicazione delle procedure disciplinari in caso di violazioni della politica e del sistema di prevenzione della corruzione; - la verifica della formazione erogata al personale (cfr. p.to 7.3); - la conduzione di interviste al personale per misurare la consapevolezza e la conoscenza della politica aziendale in materia di prevenzione della corruzione; - lo svolgimento di indagini di clima sul personale volte a comprendere se il tema anticorruzione è percepito, riconosciuto e affrontato nell'organizzazione; - laddove fattibile, un confronto tra eventuali segnalazioni ricevute e le azioni messe in atto dall'organizzazione al fine di verificare l'assenza di ritorsioni nei confronti del segnalante; - l'effettuazione di due diligence preventive sui nuovi assunti o nel caso di cambio man-

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
<p>è espressamente ricompresa la funzione compliance per la prevenzione della corruzione. L'obiettivo primario della due diligence dovrebbe essere quello di accertare preventivamente l'assenza di conflitti di interesse attuali o potenziali e di approfondire il profilo etico e reputazionale rispetto al ruolo o alla posizione che il candidato andrebbe ad assumere. L'organizzazione dovrebbe anche adottare un sistema (ad esempio, mediante l'inclusione di clausole contrattuali ad hoc) al fine di avere tempestiva notizia da parte del proprio personale del sopraggiungere di fatti o circostanze che possono determinare l'insorgere di un conflitto di interessi o una situazione di incompatibilità rispetto alla posizione o al ruolo ricoperti.</p> <p>Ai soggetti identificati "a maggior rischio" e ai componenti dell'Alta Direzione o dell'Organo Direttivo (se presente), la norma richiede di rinnovare, a cadenze ragionevoli rispetto ai livelli di rischio, il proprio impegno formale al rispetto della politica dell'organizzazione per la prevenzione della corruzione.</p> <p>In pratica, si richiede di rinnovare espressamente l'impegno assunto contrattualmente al momento dell'assunzione.</p> <p>Infine, l'organizzazione deve effettuare un riesame circa l'erogazione di bonus e incentivi sui compensi e le remunerazioni dei membri del personale considerati a rischio di corruzione superiori al livello basso, per verificare la presenza di presidi atti ad evitare che il sistema premiale favorisca la corruzione (ad esempio: quando il bonus sia legato alla conclusione di contratti con soci in affari identificati a rischio di corruzione non basso).</p>	<p>sioni, per approfondire, in relazione ai rischi di corruzione associati alla posizione o al ruolo, la presenza di conflitti di interesse o di situazioni di incompatibilità;</p> <ul style="list-style-type: none"> - la verifica sulle modalità seguite per selezionare i candidati alla posizione con rischi di corruzione superiori al livello basso (ad es. verbali di colloqui, test, etc.) e, in caso di affidamento dell'incarico per concorso, i presidi applicati per assicurare l'imparzialità, la trasparenza e l'imparzialità di giudizio sulla valutazione dei requisiti; - l'analisi dei contratti e delle lettere di assunzione del personale con le dichiarazioni di assenza di conflitti di interesse rispetto a ruoli e posizioni con rischi superiori al livello basso di corruzione e con l'impegno a comunicarli in caso di sopravvenienza; - la verifica sull'applicazione di presidi atti ad evitare il cumulo in capo ad uno stesso soggetto di più incarichi di ufficio e incarichi extra-istituzionali che potrebbero comportare un'eccessiva concentrazione di potere su un unico centro decisionale: a tal fine l'organizzazione può disciplinare in via generale i criteri di conferimento e i criteri di autorizzazione degli incarichi extra-istituzionali per assicurare l'assenza di profili di conflitto di interesse; - l'analisi delle regole dell'organizzazione (formalizzate, ad esempio, in codici etici o di comportamento) che prevedono il comportamento eticamente e giuridicamente adeguato da tenere nelle diverse situazioni critiche in cui il personale interno od esterno dell'organizzazione (soci in affari) potrebbe ritrovarsi, con l'indicazione dei riferimenti dei soggetti cui i dipendenti possono rivolgersi per chiarire eventuali dubbi o avere delucidazioni su come affrontarle (ad es. funzione di conformità, risorse umane, internal audit, etc.); - la valutazione dell'idoneità delle misure volte alla protezione dell'identità dei segnalanti di eventuali fenomeni corruttivi o elementi di rischio del sistema non adeguatamente considerati, mettendoli al riparo da eventuali fenomeni ritorsivi; - la verifica della coerenza e adeguatezza de-

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
	<p>gli MBO assegnati per il raggiungimento di obiettivi di tipo economico-finanziario; questa verifica potrebbe essere effettuata anche attraverso un confronto tra obiettivi assegnati e premi erogati per valutare l'efficacia del sistema di incentivazione.</p>
7.3 Consapevolezza e formazione	
<p>L'efficacia del sistema di gestione per la prevenzione della corruzione non può prescindere dalle persone che lavorano per l'organizzazione e, in alcuni casi, per i soci in affari.</p> <p>Non è realistico pensare che il funzionamento del sistema di controllo dei rischi di corruzione dell'organizzazione, per quanto formalmente e tecnicamente ineccepibile dal punto di vista delle regole, possa prescindere dal contributo consapevole di tutti i suoi componenti ad ogni livello.</p> <p>Le persone non solo devono astenersi dal partecipare direttamente ad atti di corruzione, ma devono essere in grado di identificare eventuali potenziali situazioni critiche e di attivare le procedure previste dal sistema di gestione stesso, fornendo ciascuno (e a partire dall'Alta Direzione) il proprio contributo per creare un clima sfavorevole alla diffusione della corruzione nell'organizzazione.</p> <p>Per questo motivo è essenziale che tutto il personale sia consapevole e formato ed è facile comprendere come la formazione rappresenti una misura (LA MISURA) organizzativa fondamentale per assicurare l'efficacia del sistema di gestione per la prevenzione della corruzione.</p> <p>I requisiti da coprire riguardano:</p> <ul style="list-style-type: none"> - volontà dell'Alta Direzione di prevenire e combattere la corruzione (politica per la prevenzione della corruzione); - i danni causati all'organizzazione della corruzione; - le circostanze in cui può avvenire la corruzione (in relazione al ruolo delle singole persone) e come riconoscere i tentativi di corruzione; - come riconoscere e affrontare le richieste di tangenti; - come prevenire la corruzione e gli indicatori chiave per la prevenzione della corruzione; - il contributo dei singoli nella prevenzione della corruzione e i benefici delle prevenzione della corruzione e delle segnalazione dei casi sospetti; 	<p>Durante l'audit, l'applicazione del presente requisito da parte dell'organizzazione dovrebbe essere valutata, oltre che mediante le attestazioni e le registrazioni relative ai percorsi formativi ed addestramenti, anche attraverso interviste dirette finalizzate a valutare l'effettivo livello di coinvolgimento e consapevolezza del personale.</p> <p>L'intervista al personale, durante tutta la conduzione dell'audit, è infatti il metodo più idoneo per verificare l'acquisizione della consapevolezza, e quindi l'efficacia di quanto attuato dall'organizzazione per soddisfare il requisito.</p> <p>Tuttavia, nel caso dei soci in affari, l'esame delle registrazioni rappresenta lo strumento per la verifica dell'applicazione del requisito. Possibili esempi di registrazioni da esaminare possono essere:</p> <ul style="list-style-type: none"> - valutazione dei fabbisogni formativi del personale e quella (eventuale) dei soci in affari con livelli di rischio superiori al livello basso; - piani della formazione, nei quali dovrebbe essere evidenziata la parte relativa ai rischi specifici di corruzione in funzione del ruolo e del processo interessato; - registrazioni relative ad attività formative concluse (dettaglio degli argomenti, personale presente, docenti e relative qualifiche ecc.).

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
<p>- le conseguenze derivanti dalla mancata o dalla non corretta applicazione del sistema di gestione per la prevenzione della corruzione;</p> <p>- come e a chi segnalare sospetti casi di corruzione.</p> <p>Una volta raggiunto un adeguato livello di formazione e consapevolezza, questo deve essere mantenuto attraverso un piano formativo che preveda aggiornamenti a intervalli regolari definiti in funzione dei ruoli e del rischio di corruzione a cui questi sono esposti. Il programma di formazione deve essere aggiornato periodicamente secondo necessità.</p> <p>In funzione dei risultati della valutazione del rischio di corruzione potrebbe essere necessario (e ragionevole) prevedere attività di formazione e sensibilizzazione anche nei confronti di soci in affari la cui attività espone l'organizzazione a rischio di corruzione. In questi casi, secondo la norma (cfr. p.to A.9.8), si tratterebbe di veri e propri "obblighi" a carico delle terze parti, che l'organizzazione deve comunicare ai soci in affari, riversandoli, ad esempio, negli accordi contrattuali con costoro.</p>	
7.4 Comunicazione	
<p>La corretta gestione e il controllo dei flussi di comunicazione, sia interni che in ingresso/uscita dall'organizzazione sono strumenti essenziali per assicurare il funzionamento e l'efficacia del sistema e per la diffusione di un clima sfavorevole alla corruzione.</p> <p>Il requisito richiede all'organizzazione di definire un vero e proprio "piano della comunicazione" identificando cosa, quando, con chi, come comunicare e definendo i responsabili di queste comunicazioni. Sotto tale profilo è importante individuare gli stakeholder con aspettative rilevanti rispetto al sistema di gestione per la prevenzione della corruzione in modo da rispondere adeguatamente a ogni richiesta, ovvero per attivare iniziative di comunicazione per migliorare i rapporti con il contesto esterno e, conseguentemente, ridurre certi livelli di rischio di corruzione ad esso associati.</p> <p>In particolare, la norma richiede che la politica dell'organizzazione per la prevenzione della corruzione sia messa a disposizione di tutto il personale e dei soci in affari in generale, e che sia comunicata espressamente (e con canali adeguati) a tutti i membri del personale e ai soci in affari con livelli di rischio</p>	<p>Possibili evidenze da considerare per valutare la conformità al requisito riguardano:</p> <ul style="list-style-type: none"> - l'applicazione e l'efficacia delle procedure di comunicazione interna con riferimento ad aspetti rilevanti ai fini del sistema di gestione per la prevenzione e il controllo dei rischi di corruzione; - la mappatura dei requisiti relativi ad "esigenze ed aspettative" delle terze parti cui l'organizzazione deve rispondere comunicando in uscita o fornendo risposte a richieste in ingresso; - la rilevazione, l'aggiornamento e la sorveglianza degli obblighi di comunicazione previsti ex lege (ad esempio, verso l'autorità nazionale competente in materia di anti corruzione, in Italia ANAC) e di quelli assunti volontariamente in forza di accordi, convenzioni o protocolli nei confronti di terze parti rilevanti (ad esempio, i flussi informativi nei confronti di organi di sorveglianza (n Italia, l'OdV ai sensi del D.lgs. 231/2001); - la definizione dei compiti e delle responsabi-

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
<p>di corruzione superiori al livello basso.</p> <p>Tale disposizione è coerente con quanto previsto in altri punti della norma circa l'impegno al rispetto della politica dell'organizzazione, richiesto ai membri del personale (cfr. p.to 7.2.2.2) e ai soci in affari (cfr.p.to 8.6) con rischi superiori al livello basso.</p>	<p>lità per le comunicazioni verso l'esterno, con l'attribuzione, ove necessario, di adeguati poteri (ad esempio, mediante deleghe);</p> <ul style="list-style-type: none"> - l'eventuale elaborazione di un piano/strategia sia per comunicare l'attuazione della politica per la prevenzione della corruzione da parte dell'organizzazione sia per affrontare e gestire eventuali situazioni di crisi derivanti dalla diffusione di notizie di pubblico dominio riguardanti il coinvolgimento di esponenti dell'organizzazione in fatti di corruzione.
7.5 Informazioni documentate	
<p>Anche la norma UNI ISO 37001, come tutte le norme che hanno alla loro base il sistema del risk based approach, prevede per la sua attuazione, la corretta gestione dei supporti e – più specificamente – delle informazioni documentate che sono raccolte dall'organizzazione per l'attuazione del sistema.</p> <p>Proprio con il fine di suggerire all'organizzazione situazioni di fatto che possono verificarsi nel corso dell'implementazione e del mantenimento del sistema di gestione adottato, la norma UNI ISO 37001 definisce - mediante classificazione precisa e coerente – quali documenti e registrazioni il sistema di gestione per la prevenzione della corruzione di una organizzazione debba mantenere e conservare.</p> <p>La norma UNI ISO 37001 specifica espressamente nell'ambito dei singoli requisiti quali documenti e registrazioni debbano essere predisposti e conservati.</p> <p>Oltre a questi documenti e registrazioni, l'organizzazione deve stabilire quali ulteriori documenti predisporre al fine di rendere più efficaci i controlli dei rischi e di migliorare la diffusione di prassi, procedure e comportamenti coerenti con la politica per la prevenzione della corruzione.</p> <p>Poiché le registrazioni servono per tracciare l'avvenuto svolgimento di un'attività (ad es. controlli, due diligence), l'organizzazione deve assicurare adeguate misure per la loro conservazione.</p> <p>La gestione delle informazioni secondo la logica prevista dalla norma UNI ISO 37001 prevede l'applicazione di un accurato processo di gestione, controllo e archiviazione che deve rendersi sinergico con altri eventuali sistemi di gestione dell'organizzazione.</p> <p>Anche le informazioni documentate di origine esterna, ritenute necessarie dall'organizzazione per la pianificazione e per il funzionamento del sistema di</p>	<p>Tra i fattori da esaminare per la valutazione della conformità possono rientrare:</p> <ul style="list-style-type: none"> - la sussistenza di documenti e registrazioni previsti come "obbligatori" dalla norma UNI ISO 37001 quali ad esempio la politica per la prevenzione della corruzione e le modalità di diffusione e divulgazione all'interno ed all'esterno dell'organizzazione; - il sistema di controllo dei documenti che comprende l'identificazione e la descrizione (per esempio titolo, data, autore o numero di riferimento), il formato (per esempio lingua, versione del software, grafica) e il supporto utilizzato (per esempio cartaceo, elettronico), riesame e approvazione in merito all'idoneità e all'adeguatezza dei documenti; - le modalità di revisione periodica dei documenti, quali ad esempio le politiche, le procedure e i controlli del sistema di gestione per la prevenzione della corruzione, i risultati della valutazione del rischio di corruzione; - le modalità per l'archiviazione e la conservazione dei documenti e delle registrazioni e per la protezione delle informazioni in essi contenute. <p>Se l'organizzazione è tenuta ad applicare altri sistemi di prevenzione della corruzione (ad es., in Italia, Piani Triennali Prevenzione Corruzione o Modelli Organizzativi ai sensi del D.lgs. 231/2001), occorrerà tenere in considerazione il livello di integrazione e di coerenza dei documenti e delle registrazioni relativi a tali sistemi, con quanto previsto dai requisiti della norma UNI ISO 37001.</p>

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
<p>gestione per la prevenzione della corruzione, devono essere opportunamente identificate e controllate. L'organizzazione deve inoltre regolamentare gli accessi alle informazioni documentate definendo i diversi livelli di autorità richiesti per prenderne visione o per modificarli.</p>	
8 ATTIVITA' OPERATIVE	
8.1 Pianificazione e controllo operativi	
<p>L'Organizzazione deve stabilire, attuare, tenere sotto controllo e mantenere i processi necessari per soddisfare i requisiti del sistema di gestione per la prevenzione della corruzione e attuare le azioni identificate nelle fasi di analisi e valutazione dei rischi.</p> <p>Questo requisito riguarda l'attuazione dei controlli sui processi e sulle misure di prevenzione che l'organizzazione ha pianificato in seguito agli esiti della valutazione dei rischi di cui al p.to 4.5.1. Esso prevede che l'organizzazione:</p> <ul style="list-style-type: none"> - stabilisca i criteri per i processi ovvero le modalità di conduzione delle attività tali da contenere i rischi di corruzione e da soddisfare i requisiti della norma UNI ISO 37001; - attui dei controlli sulla conformità dei processi ai criteri identificati per contenere i rischi di corruzione; - conservi traccia documentata degli esiti di questi controlli in modo da avere evidenza che i processi vengano svolti come pianificato (per contenere i rischi di corruzione). <p>Pertanto l'organizzazione deve pianificare e attuare i controlli e le misure più idonee a contenere i rischi specifici di corruzione.</p> <p>Il sistema di controllo deve comprendere anche le procedure e i controlli specifici previsti dai requisiti del capitolo 8 della norma UNI ISO 37001. Questi sono:</p> <ul style="list-style-type: none"> - due diligence (8.2) - controlli finanziari (8.3) - controlli non finanziari (8.4) - controlli attuati da parte di organizzazioni controllate e soci in affari (8.5) - impegni per la prevenzione della corruzione (8.6) - procedure relative a omaggi, donazioni, liberalità e altri benefits (8.7) - procedure per la gestione delle segnalazioni (8.9) - procedure per la gestione di indagini interne (8.10). <p>Occorre sottolineare che il set di controlli previsti dalla norma è tassativo ma non esaustivo. L'orga-</p>	<p>La verifica della conformità viene svolta mediante analisi a campione di documenti/registrazioni ed interviste ai responsabili/addetti dei processi rilevati e valutati a rischio di corruzione in applicazione dei relativi requisiti.</p> <p>La verifica in campo non può limitarsi all'analisi puntuale della conformità formale dei documenti e delle registrazioni, ma deve prendere in considerazione l'operatività del processo a rischio (e delle sue eventuali interazioni) allo scopo di valutare se i criteri di controllo stabiliti dall'organizzazione siano effettivamente applicati e contribuiscano a contenere i rischi.</p> <p>Per raggiungere questo obiettivo vi è la necessità di disporre di:</p> <ul style="list-style-type: none"> - criteri di campionamento idonei a fornire informazioni rappresentative ai fini del giudizio di conformità; - tempi adeguati per l'effettuazione delle interviste in ragione dei livelli di rischio dei processi soggetti ai controlli; - diretto coinvolgimento dei responsabili e/o addetti incaricati di processi a rischio di corruzione. <p>E' opportuno valutare preliminarmente l'impostazione complessiva del sistema dei controlli pianificato e attuato dall'organizzazione al fine di verificarne la coerenza con gli esiti della valutazione dei rischi di corruzione.</p> <p>A ciascun rischio identificato e valutato come non trascurabile dovrebbe corrispondere una misura di controllo. La programmazione dei controlli dovrà dare evidenza dei tempi e delle responsabilità per la loro attuazione e sorveglianza.</p> <p>Occorre infine valutare come l'organizzazione gestisce i documenti e le registrazioni che</p>

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
<p>nizzazione potrebbe infatti identificare misure ulteriori rispetto a quelle sopra elencate purché idonee a contenere i rischi. In ogni caso, il processo di gestione del rischio di corruzione della norma UNI ISO 37001 richiede di evidenziare la correlazione chiara ed univoca tra rischio identificato e valutato, i controlli programmati e attuati per contenere questo rischio, comprese le responsabilità di questi controlli e la sorveglianza sull'attuazione dei controlli.</p> <p>Il sistema dei controlli inoltre non è "statico" ma "dinamico". L'organizzazione deve tenere monitorare le modifiche programmate e, valutato preventivamente l'impatto di queste modifiche sui rischi di corruzione, apportare gli interventi atti a contenere eventuali aggravati di rischio.</p> <p>Nel caso di cambiamenti imprevisti (o involontari) deve valutare le ricadute in termini di rischi di corruzione e rivedere tempestivamente l'adeguatezza dei controlli in essere per mitigare gli (eventuali) effetti negativi di questi cambiamenti.</p>	<p>attestino che i controlli siano stati effettuati come programmato.</p> <p>Nella parte della norma UNI ISO 37001 che riguarda i controlli, come per quella che tratta l'analisi e la valutazione dei rischi, risultano più evidenti i profili di integrazione del sistema volontario con altri strumenti di prevenzione e controllo dei rischi di corruzione adottati dall'organizzazione (ad es. modelli organizzativi ai sensi del D.Lgs. 231/2001, piani triennali di prevenzione della corruzione, compliance programs anti bribery).</p> <p>In questi casi, la verifica riguarderà gli stessi controlli, procedure e regole, con i relativi documenti e registrazioni.</p> <p>Nel caso di duplicazione di controlli previsti da sistemi diversi a presidio del medesimo rischio, si dovrebbe valutare con attenzione l'effettiva capacità dell'organizzazione di tenere sotto controllo questi rischi. Analoga considerazione andrebbe fatta nel caso opposto, quando vi sia evidenza di controlli e procedure del sistema UNI ISO 37001 disallineati con quelli previsti da altri sistemi aziendali a presidio del medesimo rischio.</p> <p>In conseguenza di modifiche programmate e/o cambiamenti inaspettati, occorre verificare se siano applicate procedure per identificare, analizzare e trattare gli eventi che possono avere effetti sui rischi di corruzione e per apportare eventuali modifiche al sistema dei controlli idonee a prevenirli o a contenere gli effetti negativi del loro accadimento.</p>
8.2 Due Diligence	
<p>Secondo la definizione della norma UNI ISO 37001 (cfr. p.to 3.30 della norma - A.10.1 della Guida sull'utilizzo) la due diligence è un processo per approfondire natura ed estensione dei rischi di corruzione e rappresenta anche un controllo "aggiuntivo e mirato" per mitigare i rischi (per questo motivo è inclusa tra i "controlli" del par. 8 della norma).</p> <p>La due diligence può riguardare categorie di transazioni, progetti, attività, soci in affari e membri del personale dell'organizzazione per le quali la valutazione dei rischi (cfr. p.to 4.5.1) abbia rilevato un livello di rischio di corruzione superiore al basso.</p> <p>L'obiettivo della due diligence è quello di suppor-</p>	<p>Pur non essendo esplicitamente richiesto dal requisito, è opportuno che le modalità operative della due diligence siano documentate in apposita procedura (o linea guida) al fine di facilitarne la diffusione e migliorare l'efficacia del controllo sulla sua applicazione.</p> <p>Dovrebbe essere verificato il campo di applicazione della due diligence con la mappatura delle categorie di soci in affari che operano per conto dell'organizzazione e delle tipologie di operazioni (es. acquisizioni, accordi commerciali o di partnership, sponsorizzazioni etc.) con livelli di rischio di corruzione su-</p>

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
<p>tare il processo decisionale dell'organizzazione con maggiori informazioni sotto il profilo dei rischi di corruzione che essa potrebbe trovarsi ad affrontare nell'ambito delle categorie sopracitate.</p> <p>Il percorso metodologico indicato dalla norma è il seguente:</p> <ul style="list-style-type: none"> - nell'ambito della valutazione dei rischi l'organizzazione identifica le categorie di transazioni, progetti, attività e soci in affari con rischi di corruzione superiori al livello basso; - per queste categorie si prevede l'effettuazione di una due diligence diretta a ottenere informazioni più approfondite per valutare il rischio di corruzione; - la due diligence deve essere ripetuta a intervalli pianificati in modo da assicurare l'aggiornamento delle informazioni. <p>Il requisito contiene un'importante precisazione (Nota 1 al p.to 8.2) da considerare anche ai fini della valutazione di conformità: l'organizzazione potrebbe stabilire di non procedere con la due diligence dove non sia necessario, ragionevole o congruo. Questa decisione dovrebbe essere ben motivata alla luce degli esiti della valutazione dei rischi.</p> <p>La norma non stabilisce le modalità di esecuzione della due diligence che l'organizzazione deve definire in funzione della propria capacità di ottenere sufficienti informazioni, dei costi per reperire queste informazioni e dell'entità dei rischi derivanti, ad esempio, dalla relazione con i soci in affari.</p> <p>Con riferimento a questi ultimi la "Guida all'utilizzo" (allegato A) riporta, a titolo di esempio, alcuni elementi che potrebbe essere utile approfondire ai fini della valutazione dei rischi:</p> <ul style="list-style-type: none"> - esercizio legittimo dell'attività da parte del socio in affari in base alle normative vigenti (anche fiscali); - competenze, esperienza e professionalità del socio in affari, comprese le risorse necessarie, per l'esecuzione dell'incarico che si intende affidare; - notizie di pubblico dominio che riguardino il coinvolgimento del socio in affari in atti di corruzione, condotte fraudolente o illeciti analoghi; - esistenza di procedimenti a carico del socio in affari per fatti di corruzione o illeciti analoghi; - adozione da parte del socio in affari di un sistema per la prevenzione dei rischi di corruzione; - notizie e informazioni relative ad azionisti e Alta Direzione dei soci in affari; - struttura e forma del contratto o degli incarichi e 	<p>periori al basso.</p> <p>A tale proposito è importante sottolineare che "i soci in affari" da prendere in considerazione sono terze parti che, operando per conto dell'organizzazione, possono esporre quest'ultima a rischi di corruzione. Andrà quindi verificato se l'organizzazione ha analizzato quali siano i rischi di corruzione connessi alle attività del socio in affari (ad esempio, con riferimento a rapporti con pubblici funzionari) e ha determinato se e in quale misura possano coinvolgere la responsabilità dell'organizzazione stessa.</p> <p>Inoltre, devono essere chiaramente indicati i soggetti dell'organizzazione tenuti ad applicare le procedure di due diligence in base non solo al loro ruolo o alla posizione (es. procurement, addetti alla rete di vendita, alle relazioni esterne, etc.) ma anche in relazione alle responsabilità assunte "di fatto" per la gestione dei rapporti con soci in affari qualificabili "a rischio non basso".</p> <p>Occorre quindi verificare che sia stato specificato e comunicato a tutti gli interessati il divieto di concludere nuovi accordi (o modifiche di essi) o instaurare relazioni con le categorie a rischio in mancanza di una preventiva due diligence.</p> <p>La due diligence potrebbe richiedere gradi di approfondimento, tempistiche e iter di validazione diversi in funzione dei profili di rischio associati alla categoria.</p> <p>Occorre verificare se la due diligence si stata applicata non solo ai soci in affari con i quali l'organizzazione intende intraprendere un rapporto di business, ma anche a quelli (con livelli di rischio superiori al livello basso) già acquisiti sulla base di relazioni o accordi preesistenti.</p> <p>Nel caso di nuovi appaltatori o fornitori di beni o servizi, la raccolta di informazioni dovrebbe essere integrata con il processo di qualifica/selezione del socio in affari.</p> <p>L'organizzazione dovrebbe aver considerato nell'ambito di applicazione della due diligence anche la verifica sulla sussistenza di motivi di esclusione degli operatori economici dalle procedure di appalto, se previsti da norme</p>

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
<p>delle modalità di pagamento.</p> <p>Per il personale la due diligence è prevista dal requisito 7.2.2.2: è richiesto all'organizzazione di integrare nelle procedure di assunzione (o per un cambio di mansioni) una due diligence proporzionata ai rischi associati al ruolo.</p>	<p>di legge ad essa applicabili (in Italia, il D.Lgs 50/2016, cd "Codice degli Appalti"). Tra queste cause di esclusione potrebbero essere infatti annoverate anche circostanze rilevanti per il sistema di prevenzione della corruzione quali condanne definitive per fatti di corruzione o illeciti analoghi, gravi illeciti professionali finalizzati a influenzare indebitamente il processo di decisione sull'affidamento dell'appalto, conflitti di interesse determinati dalla partecipazione dell'operatore economico, etc. L'obiettivo, analogo a quello della due diligence, è effettuare un approfondimento (preventivo) sul potenziale partner al fine di escludere colui o coloro che presentino profili di rischio incompatibili, in questo caso, con le finalità di legge.</p> <p>Nel caso di rapporti già esistenti, occorre effettuare un approfondimento sulla natura e sul contenuto degli accordi alla base di questi rapporti, sulle modalità di esecuzione degli stessi, sulla forma di pagamento dei compensi. Le modalità di effettuazione della due diligence dipendono dalle capacità dell'organizzazione (anche in termini di costi) e sono proporzionate all'entità dei rischi di corruzione da affrontare.</p> <p>L'obiettivo della norma UNI ISO 37001 non è quello di costringere le organizzazioni a predisporre strumenti costosi, burocratici e, in ultima analisi, del tutto inutili ai fini della gestione dei rischi di corruzione. Occorre quindi che l'organizzazione abbia correttamente identificato strumenti idonei ed efficaci ad approfondire la valutazione dei rischi di corruzione e ad identificare eventuali criticità rispetto a quanto oggetto di due diligence.</p> <p>Ciò premesso, la due diligence sui soci in affari può avvenire con l'ausilio di questionari, con l'acquisizione di certificati o attestazioni, mediante la consultazione di banche dati, elenchi, white list, siti web, etc.</p> <p>L'organizzazione deve analizzare, trattare e gestire le informazioni raccolte con la due diligence in modo da avere un quadro sufficientemente chiaro circa gli eventuali rischi che possono determinarsi avvalendosi dell'operato di terzi, o dall'acquisizione di asset (aziende o parti di esse, partecipazioni, etc.),</p>

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
	<p>o intraprendendo nuovi progetti o attività. Nel caso in cui la due diligence abbia riscontrato particolari criticità, l'elemento di attenzione (o "red flag") deve essere comunicato a tutti coloro che hanno la responsabilità di approfondire il caso e di prendere decisioni in merito alla prosecuzione dell'affare o della relazione con il socio in affari, ovvero di sospendere o anche di abbandonarli.</p> <p>Poiché circostanze, fatti e situazioni analizzati con la due diligence possono cambiare nel corso del tempo, determinando anche una variazione dei livelli di rischio individuati, occorre che le procedure dell'organizzazione prevedano anche che la due diligence sia ripetuta a intervalli di tempo predefiniti e in ogni caso aggiornata a seguito di modifiche rilevanti per i rischi di corruzione.</p>
<h3>8.3 Controlli finanziari</h3>	
<p>L'Organizzazione deve prevedere modalità di gestione (controlli) delle risorse finanziarie idonee ad evitare il rischio di corruzione.</p> <p>Tali controlli raggruppano i sistemi e le prassi gestionali attuate dall'organizzazione per gestire in modo regolare le transazioni finanziarie (cfr. p.to 8.1).</p> <p>Le modalità di attuazione dei controlli finanziari saranno diverse in ragione delle dimensioni e delle tipologie di contratti gestiti e in relazione al tipo di organizzazione (ad es. società quotate, società che operano nell'ambito di contratti con la PA, società pubbliche).</p> <p>Questi controlli devono garantire che le risorse finanziarie dell'organizzazione siano utilizzate in modo corretto ed appropriato, siano protette e registrate e che i pagamenti siano effettuati solo verso soci in affari a fronte di una attività legittima.</p> <p>La maggior parte delle organizzazioni dispone già di controlli finanziari conformi a standard contabili stabiliti da norme nazionali e, in genere, lo scopo di questi controlli può essere più ampio rispetto alla prevenzione della corruzione (es. le organizzazioni quotate devono conformarsi ai requisiti di controllo finanziario del mercato azionario).</p> <p>Nel progettare e implementare il sistema di gestione, l'organizzazione deve valutare in che misura i</p>	<p>I controlli finanziari dovranno essere stabiliti sulla base di responsabilità, deleghe e procure presenti e in considerazione di quanto emerso dalla analisi dei rischi (cfr. p.to 4.5).</p> <p>La verifica della conformità è svolta tramite analisi a campione di documenti/registrazioni relativi alla gestione dei flussi finanziari, quali a titolo esemplificativo:</p> <ul style="list-style-type: none"> - gestione del ciclo attivo (incassi) e del ciclo passivo (pagamenti e riversamenti) - gestione dei flussi finanziari relativi ai rapporti consulenziali; - gestione dei flussi finanziari con la Pubblica Amministrazione; - gestione dei fondi cassa (verifica circa la corretta riconciliazione, contabilizzazione e reintegrazione); - gestione dei conti correnti bancari e dei rapporti con gli istituti bancari e finanziari (apertura e chiusura, riconciliazione degli estratti conto). <p>Esempi di controlli finanziari da verificare per ridurre il rischio di corruzione comprendono:</p> <ul style="list-style-type: none"> - la separazione di responsabilità tra chi avvia un pagamento e chi lo approva (es. il responsabile produzione richiede l'acquisto e il responsabile amministrativo ne ordina il pagamento);

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
<p>controlli finanziari esistenti aiutino a ridurre i rischi di corruzione. Nel caso in cui non siano sufficienti a contenere i rischi, l'organizzazione dovrebbe considerare se rafforzare questi controlli possa contribuire a ridurre i rischi valutati, migliorando quindi i controlli esistenti in misura ragionevole e proporzionata. La guida (p.to A.11) fornisce alcuni esempi di controlli finanziari che possono ridurre il rischio di corruzione.</p>	<ul style="list-style-type: none"> - la definizione di livelli gerarchici con responsabilità crescenti in modo che il pagamento di transazioni elevate sia affidato a livelli gerarchici elevati (es. coerenza dei poteri di spesa rispetto alle soglie dei poteri di firma conferiti ovvero la rispondenza degli importi previsti da contratti quadro/ordini di acquisto con i poteri di firma stabiliti); - la verifica che il pagamento per il lavoro o i servizi effettuati siano autorizzati secondo i pertinenti livelli di responsabilità, ad esempio che il pagamento sia autorizzato a fonte della effettiva prestazione; - la richiesta di almeno due diverse funzioni sulle approvazioni di pagamento; - la richiesta della documentazione di supporto appropriata che garantisca adeguata tracciabilità del flusso autorizzativo (ad es. sulla sequenza preventivo-fattura-pagamento); - la restrizione dell'uso del contante e l'attuazione di metodi efficaci di controllo del contante; - la richiesta che tutte le transazioni finanziarie siano adeguatamente classificate e le descrizioni dei pagamenti nei conti siano accurate e chiare; - l'attuazione di un riesame gestionale periodico delle transazioni finanziarie significative e attuazione di audit finanziari periodici e indipendenti. In questo caso è necessario prevedere regole di avvicendamento della persona o dell'organizzazione a cui sono affidati i controlli indipendenti. <p>La verifica del requisito non ha il medesimo obiettivo degli audit finanziari, ma dovrà verificarne l'effettuazione, anche in conformità agli obblighi di legge, laddove presenti.</p> <p>Occorre verificare se le procedure di gestione delle risorse finanziarie assicurino:</p> <ul style="list-style-type: none"> - la tracciabilità dei flussi, cioè la possibilità di ricostruire ex post il percorso decisionale e formale dei flussi (chi ha pagato, chi è stato pagato, con quale mezzo di pagamento, come e dove è stato prelevato); - la documentazione dei flussi finanziari, quali ad esempio, registrazioni della forma di pagamento e dei giustificativi (chi ha auto-

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
	<p>rizzato/disposto il flusso, chi è il beneficiario e la causale).</p> <p>Possibili indicatori di anomalia (red flags) possono essere:</p> <ul style="list-style-type: none"> - ordini di pagamento nei confronti di soggetti non identificabili, non presenti in anagrafica; - non piena corrispondenza tra il nome del fornitore e l'intestazione del conto su cui fare il pagamento; - incassi da soggetti non presenti in anagrafica e non giustificati dalla presenza di un credito in contabilità o supportati da adeguata documentazione giustificativa; - pagamenti su conti cifrati e/o utilizzo istituti di credito privi di insediamenti fisici (cd. Istituti virtuali) e/o utilizzo del contante (ad eccezione della piccola cassa) o altro strumento finanziario al portatore; - versamenti a società residenti in paradisi fiscali e/o paesi inclusi in black list.
8.4 Controlli non finanziari	
<p>L'organizzazione deve definire i controlli non finanziari in modo che i rischi connessi alla corruzione nell'ambito delle varie attività possano essere gestiti adeguatamente.</p> <p>Attraverso la mappatura dei processi sarà possibile analizzare lo stato attuale e i presidi in essere ed individuare le misure da adottare per contrastare comportamenti illeciti e di conseguenza abbassare la soglia del rischio.</p> <p>Il requisito contiene la precisazione (Nota 1) che ogni transazione, attività o relazione con soci in affari può essere soggetta sia a controlli finanziari sia non finanziari.</p> <p>Ciò comporta che nella identificazione e pianificazione dei controlli non finanziari si deve anche tenere conto degli effetti di altri controlli (come i controlli finanziari), in quanto l'effetto cumulativo può ridurre il rischio di corruzione a un livello accettabile.</p>	<p>Come per i controlli finanziari, anche i controlli non finanziari dovranno essere stabiliti sulla base di responsabilità, deleghe e procure presenti e in considerazione di quanto emerso dall'analisi dei rischi (cfr. p.to 4.5 e p.to 8.1). La verifica della conformità è svolta mediante analisi a campione di documenti/registrazioni ed interviste ai responsabili/addetti dei processi rilevanti.</p> <p>Occorre verificare che il sistema dei controlli assicuri che le attività di processo siano eseguite e controllate in coerenza con i risultati dell'analisi del rischio.</p> <p>Anche sulla base degli esempi forniti dalla "Guida all'utilizzo" (A.12), e sempre che i controlli contribuiscano a ridurre i rischi, l'applicazione del requisito potrebbe essere verificata con riferimento a:</p> <ul style="list-style-type: none"> - mappatura delle responsabilità dei centri di acquisto all'interno dell'organizzazione, compresa l'attribuzione degli occorrenti poteri di firma; - livello di diffusione (all'interno e all'esterno) delle politiche di procurement e di controllo

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
	<p>dell'organizzazione che dovrebbero comprendere principi e linee guida aziendali per la lotta e la prevenzione della corruzione;</p> <ul style="list-style-type: none"> - procedure per l'approvvigionamento differenziate a seconda dell'oggetto dell'acquisizione (lavori, beni, servizi, consulenze etc.), delle soglie di valore del contratto e della natura delle controparti (pubblica o privata); - procedure di selezione di appaltatori, sub-appaltatori, fornitori e consulenti che devono considerare anche gli esiti delle due diligence in fase di preselezione; - programmazione degli acquisti e budget di spesa; - tracciabilità delle diverse fasi del processo di approvvigionamento (anche mediante sistemi informativi) con le registrazioni delle diverse operazioni; - verifiche sulla legittimità delle richieste di acquisto in relazione ai fabbisogni dell'organizzazione, - verifiche sulla congruità del corrispettivo rispetto al servizio o al bene in contratto; - monitoraggio sull'effettiva erogazione delle prestazioni in conformità alle specifiche contrattuali (ad es. stato avanzamento lavori, collaudo, benessere merce in entrata, modalità di pagamento, rispetto delle scadenze); - monitoraggio di varianti ai contratti, proroghe e deroghe alle procedure di acquisto al fine di valutarne legittimità, necessità e fondatezza; - previsione di supervisione e di autorizzazione di livelli gerarchici/funzionali adeguati nel caso di operazioni straordinarie, di deroghe e/o proroghe che possono determinare rischi di corruzione significativi; - modalità di protezione e di accesso ai dati relativi alle offerte ricevute (es. sui prezzi); - applicazione di misure organizzative relative al personale quali, ad esempio, procedure di rotazione dei dipendenti che operano nei processi maggiormente a rischio; - adozione di codici etici e codici di comportamento recanti disposizioni settoriali per fronteggiare situazioni di rischio specifico, ad esempio per particolari tipologie profes-

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
	<p>sionali oppure per condotte standard da seguire in particolari situazioni come nel caso di rapporti/contatti con Pubblici Ufficiali ovvero di accessi presso utenze private.</p> <p>Laddove risulti ragionevole, in funzione della capacità di queste misure, contenere i rischi di corruzione associati all'operazione, i controlli potrebbero riguardare inoltre:</p> <ul style="list-style-type: none"> - l'introduzione della prassi secondo cui l'affidamento di appalti per servizi e forniture avvenga solo in seguito a una procedura "aperta" che richieda la valutazione di almeno tre preventivi; - l'attuazione della separazione di funzioni in modo che la redazione e l'approvazione dei documenti di gara, l'aggiudicazione dell'affidamento e la verifica circa l'esecuzione del contratto siano attribuite a soggetti distinti; - la previsione che i soggetti coinvolti nella redazione della documentazione di gara debbano sottoscrivere specifiche dichiarazioni in cui attestino l'assenza di interessi personali in relazione allo specifico oggetto della gara; - l'introduzione della previsione secondo cui i contratti e i documenti che modificano le condizioni contrattuali relativamente ad un appalto già in esecuzione o che certificano l'avvenuta esecuzione del lavoro, del servizio o della fornitura previsti dal contratto, debbano essere approvati e firmati da almeno due soggetti; - l'adozione di direttive e linee guida interne che disciplinino la corretta conservazione della documentazione di gara per un tempo congruo al fine di consentire verifiche successive, prevedendo ad esempio la costituzione di appositi archivi (fisici e/o informatici) per la custodia della documentazione. <p>Con riferimento ai controlli non finanziari e in particolare a quelli relativi al processo di approvvigionamento, l'organizzazione che già attua un sistema di gestione in conformità alla norma ISO 9001 potrà agevolmente considerare di integrare le procedure del sistema qualità con i controlli sui rischi di corruzione previsti dalla norma UNI ISO 37001.</p> <p>Laddove alcuni dei controlli sopra descritti siano invece obbligatori per legge per talune</p>

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
	<p>tipologie di organizzazioni (in Italia, ad esempio, per gli enti della Pubblica Amministrazione), essi dovranno essere identificati, gestiti e monitorati come requisiti di legge ai sensi della norma UNI ISO 37001.</p>
<h3>8.5 Attuazione dei controlli da parte dei soci in affari</h3>	
<p>Secondo la definizione della norma UNI ISO 37001 (cfr. p.to 3.26) i “soci in affari” sono terze parti con le quali l’organizzazione ha o progetta di stabilire una relazione commerciale di qualsiasi tipo. Non tutte le terze parti sono quindi soci in affari. La definizione di “affari”, infine, deve essere intesa in senso lato, includendo tutte le attività che fanno capo all’organizzazione e che sono pertinenti ai suoi scopi, e che pertanto non necessariamente presuppongono sempre una “relazione commerciale”.</p> <p>Per comprendere quali siano i soci in affari che l’organizzazione deve prendere in considerazione occorre riferirsi al significato di “corruzione” secondo la UNI ISO 37001. Questo include anche i rischi di corruzione (sia dal lato attivo che passivo) determinati dai soci in affari che operano, o che potrebbero operare, per conto dell’organizzazione.</p> <p>Dagli esempi della “Guida all’utilizzo” è possibile comprendere le due tipologie di rischi di corruzione, attiva e passiva, che l’organizzazione dovrebbe considerare con riferimento alle attività svolte dai soci in affari:</p> <p>1) dal lato attivo, quando il socio in affari (es. un partner in una joint venture, una controllata, la controllante, una società del gruppo che gestisce servizi in outsourcing per l’organizzazione, un agente, un consulente) agisce nei confronti di soggetti esterni (ad es. pubblici ufficiali, potenziali clienti) per conto dell’organizzazione;</p> <p>2) dal lato passivo, quando il socio in affari (ad es. fornitore, cliente) agisce nei confronti dell’organizzazione per ottenere vantaggi indebiti.</p> <p>L’organizzazione deve individuare i soci in affari (in senso lato, come spiegato in precedenza) con i quali ha o progetta di avere “relazioni commerciali” e transazioni (con rischi, di norma, di corruzione passiva). Tra i soci in affari deve identificare anche coloro che svolgono (o potrebbero svolgere) attività per conto della medesima dalle quali potrebbero derivare rischi di corruzione attiva.</p> <p>La norma UNI ISO 37001 fornisce diversi esempi di</p>	<p>In modo schematico, le evidenze per verificare la conformità a questo requisito dovrebbero, in sintesi, riguardare:</p> <ul style="list-style-type: none"> - l’individuazione dei soci in affari, nell’ambito del proprio contesto, tra le terze parti rilevanti per il sistema di gestione per la prevenzione della corruzione; - l’individuazione delle società e degli enti di cui l’organizzazione detiene il controllo, considerata la legislazione dello Stato (o degli Stati) presso il quale viene applicato lo standard UNI ISO 37001; - l’analisi e la valutazione del livello di rischio di corruzione (attiva e passiva) dei soci in affari che operano per conto dell’organizzazione; - la mappatura (per categoria) dei soci in affari con livello di rischio superiore al basso ai fini dell’applicazione dei requisiti sulla due diligence, sui controlli per la prevenzione della corruzione e sugli impegni per la prevenzione della corruzione; - la definizione di una procedura che stabilisca termini e modalità per l’effettuazione di due diligence (preventive) ogniqualvolta si determini l’occasione di instaurare una relazione o una transazione con soci in affari a rischio di corruzione; - l’applicazione della due diligence anche su rapporti e transazioni con soci in affari a rischio, già in essere sulla base di contratti/incarichi esistenti; - la diffusione di queste procedure a tutti i membri dell’organizzazione che potrebbero avere occasione di instaurare una relazione con soci in affari a rischio superiore al livello basso; - la disponibilità di informazioni (in base alla due diligence o al riesame dei contratti esistenti) circa i controlli attuati dal socio in affari per contenere i rischi di corruzione;

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
<p>soci in affari, a titolo non esaustivo: clienti, acquirenti, partner in joint venture e in consorzi, fornitori, appaltatori, sub-appaltatori, consulenti, venditori, agenti, rappresentanti, distributori, intermediari e investitori. Rispetto a ciascuna di queste categorie di soggetti l'organizzazione deve preliminarmente rendersi conto se e in quali circostanze l'attività del socio in affari possa determinare rischi di corruzione e, come spiegato in precedenza, in presenza di livelli di rischio non trascurabili, procedere a un approfondimento del rischio (o due diligence).</p> <p>In sintesi, il p.to 8.5 richiede all'organizzazione di attivare procedure affinché i soci in affari più a rischio, attivino propri controlli sui rischi di corruzione.</p> <p>Il primo fattore da considerare a tal proposito è il livello di influenza che l'organizzazione è in grado di esercitare sul socio in affari. In presenza di uno scarso livello di influenza sarà ben difficile richiedere ed ottenere dal socio in affari un sistema di controllo sui propri rischi di corruzione.</p> <p>Risulta così più agevole comprendere la distinzione operata dalla norma UNI ISO 37001 tra soci in affari che ricadono sotto il controllo dell'organizzazione e soci in affari (con livelli di rischio superiori al basso) che non ricadono sotto il controllo dell'organizzazione. Per i primi si richiede di attuare un sistema di gestione della prevenzione della corruzione o quanto meno dei controlli sui rischi di corruzione.</p> <p>Per i secondi, non sotto il controllo dell'organizzazione, si richiede di verificare se il socio in affari attui dei controlli per la prevenzione della corruzione. Qualora non vi siano questi controlli o non sia possibile verificarne la presenza, l'organizzazione deve pretendere dal socio in affari di attuarli con riferimento al rapporto, alla transazione o all'attività che la vede coinvolta.</p> <p>Se ciò non è fattibile (ad esempio, a causa dello scarso potere di influenza contrattuale), allora l'organizzazione dovrà considerare questa circostanza nella valutazione dei rischi derivanti dalla relazione con il socio in affari e nelle decisioni con cui gestire questi rischi, applicando eventualmente quanto previsto dal requisito 8.8 che tratta, per l'appunto, la "gestione dell'inadeguatezza dei controlli per la prevenzione della corruzione".</p> <p>Un altro fattore fondamentale sottolineato dalla norma UNI ISO 37001 in merito ai controlli per la prevenzione della corruzione sui soci in affari (con-</p>	<ul style="list-style-type: none"> - nel caso in cui il socio in affari non disponga di controlli per la prevenzione della corruzione o non sia stato possibile ottenere informazioni al riguardo, le azioni svolte dall'organizzazione per richiederli e ottenerli in funzione del livello di rischio, del grado di influenza (anche contrattuale) esercitabile dall'organizzazione, dall'efficacia del sistema di controllo a contenere i rischi del socio in affari; - nel caso in cui non risulti fattibile pretendere e ottenere dal socio in affari l'attuazione di controlli sui propri rischi di corruzione, le misure compensative predisposte dall'organizzazione in assenza di tali controlli; - il riesame dei rischi di corruzione connessi alla relazione o alla transazione con il socio in affari in assenza di controlli da parte di questi ultimi e, nel caso in cui il rischio risulti non accettabile, le decisioni assunte per gestire l'inadeguatezza dei controlli da parte del socio in affari come stabilito dal successivo p.to 8.8.

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
<p>trollati o meno) riguarda la ragionevolezza, la proporzionalità e, soprattutto, l'efficacia di questi controlli a contenere i rischi di corruzione del socio in affari. Se la presenza di queste misure, o le modalità attraverso le quali vengono attuate, non contribuiscono effettivamente a contenere i rischi, ma si risolvono in un adempimento meramente formale, allora l'organizzazione dovrebbe individuare strade alternative per gestire i rischi di corruzione derivanti dalla relazione con il socio in affari.</p> <p>Infine, la norma UNI ISO 37001 chiarisce cosa si debba intendere per organizzazione "controllata" ai fini dell'applicazione del requisito: l'organizzazione detiene il controllo su un'altra organizzazione qualora controlli direttamente o indirettamente gli organi direttivi dell'organizzazione (ad esempio, tramite la maggioranza dei voti in CdA ovvero mediante la maggioranza delle quote sociali).</p>	
8.6 Impegni per la prevenzione della corruzione	
<p>L'organizzazione deve richiedere a tutti i soci in affari con livelli di rischio superiore al basso, un impegno a prevenire atti di corruzione, a proprio vantaggio o quando operi per conto dell'organizzazione (corruzione attiva).</p> <p>Il requisito della norma UNI ISO 37001 richiede anche che l'organizzazione predisponga gli strumenti necessari a cessare la relazione o la transazione con il socio in affari, nel caso in cui, questi, contravvenendo all'impegno preso, abbia posto in essere atti di corruzione a proprio vantaggio o per conto dell'organizzazione.</p> <p>Quanto sopra deve essere richiesto e previsto con riferimento alla relazione o alla transazione che si intende instaurare tra l'organizzazione e il socio in affari.</p> <p>La norma UNI ISO 37001 precisa anche che l'impegno del socio in affari andrà richiesto "se fattibile". All'atto pratico, la norma richiede di prevedere a livello contrattuale un obbligo a carico del socio in affari con i relativi rimedi in caso di inadempimento, la cui fattibilità può dipendere (ancora una volta) dal livello di influenza che l'organizzazione è in grado di esercitare nei confronti della controparte.</p> <p>Altre difficoltà applicative possono derivare dal significato che si intende attribuire alla locuzione "fatti di corruzione" ai fini di un eventuale inadempimento</p>	<p>Le evidenze a supporto della valutazione di conformità possono riguardare:</p> <ul style="list-style-type: none"> - la mappatura dei soci in affari, con rischi superiori al livello basso, cui deve essere richiesta l'assunzione di impegni alla prevenzione di atti di corruzione; - l'applicazione sistematica degli strumenti (ad es. contratti) che vincolino il socio in affari a rispettare gli impegni anti corruzione (e, se del caso, il codice etico) dell'organizzazione, con la previsione dei rimedi che in caso di inadempimento consentano all'organizzazione di cessare la relazione o la transazione; - l'effettività di queste clausole nel caso di inadempimento da parte del socio in affari, al fine di valutare se e come l'organizzazione abbia intrapreso le azioni necessarie per cessare la relazione o la transazione; il riesame della valutazione dei rischi connessi alla relazione con il socio in affari nei casi in cui non risulti fattibile richiedere l'assunzione di tale obbligo da parte del socio in affari o prevedere rimedi contrattuali idonei a consentire all'organizzazione di cessare la relazione o la transazione. <p>E' consigliabile che nelle interviste siano coin-</p>

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
<p>dell'obbligo di prevenirli. Sarebbe quindi opportuno definire in modo puntuale e "contestualizzare" l'impegno assunto dal socio in affari in modo da non comprometterne l'effettività mediante l'adozione di mere clausole di stile.</p> <p>Un eventuale diniego da parte del socio in affari ad assumere un impegno a prevenire atti di corruzione ovvero l'impossibilità di prevedere dei rimedi per l'inadempimento a tale obbligo, dovrà quindi essere considerato nell'ambito della valutazione dei rischi connessi alla relazione con il socio in affari.</p>	<p>volti, oltre ai responsabili (a vario titolo) dei rapporti con i soci in affari, anche la funzione legale (se presente) e coloro che supportano l'organizzazione per la predisposizione e la redazione dei contratti.</p>

8.7 Regali, ospitalità, donazioni e benefici simili

<p>Regali, ospitalità e donazioni, offerte o ricevute possono essere interpretate, anche erroneamente, come tentativi di corruzione. L'applicazione del requisito si estende anche ad attività indirette o trasversali come sponsorizzazioni, benefici per la comunità, partecipazione a corsi di formazione, favori personali etc. E' necessario definire una politica per la gestione delle donazioni la cui complessità varia in funzione della tipologia di organizzazione e del livello di esposizione al rischio corruzione.</p> <p>Per esempio si potrebbe imporre il divieto di accettare/offrire qualsiasi tipo di donazione/ospitalità, così come si potrebbe consentire di accettare/offrire donazioni/ospitalità di "modesta entità", in questo caso, occorre definire cosa si intenda per "modesta entità".</p> <p>Analogamente si potrebbe vietare ogni tipo di donazione a partiti politici, organizzazioni, comunità; tuttavia una organizzazione potrebbe ritenere che alcuni tipi di donazione (in particolare a comunità locali, onlus ecc...) non si configurino come tentativi di corruzione e siano efficaci azioni di marketing. In questo caso è opportuno prevedere un percorso di approvazione della donazione affiancato, eventualmente, da una due diligence sull'ente destinatario della donazione.</p>	<p>Possibili evidenze per la valutazione della conformità possono essere:</p> <ul style="list-style-type: none"> - politica per la gestione delle donazioni/omaggi/ospitalità; - criteri per la definizione di "modesta entità"; - presenza di contratti in forma scritta a supporto delle donazioni di entità rilevante o di accordi di sponsorizzazione; - verifica della effettiva destinazione di quanto oggetto di donazione o di sponsorizzazione in conformità a quanto previsto in contratto; - registrazioni relative alla formazione/sensibilizzazione al personale; - colloqui con il personale per valutare il livello di sensibilità/consapevolezza; - registrazioni relative alla gestione di donazioni a enti/comunità e relativo iter di gestione; - due diligence sul destinatario della donazione.
--	--

8.8 Gestione dell'inadeguatezza dei controlli per la prevenzione della corruzione

<p>Si tratta del requisito di chiusura del processo di controllo dei rischi di corruzione previsto dalla norma UNI ISO 37001 e rappresenta nel contempo il paradigma con cui potrebbe confrontarsi l'organizzazione per confermare la credibilità della propria politica anti corruzione con la conseguente scelta di</p>	<p>Esempi di possibili evidenze per valutare la conformità al requisito possono essere:</p> <ul style="list-style-type: none"> - valutazione della situazione esistente all'avvio del Sistema (cfr. p.to 4.5); - valutazione preventiva del rischio corruzione per nuove attività, commesse, contratti,
---	---

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
<p>applicare un sistema volontario per la prevenzione della corruzione.</p> <p>Possono infatti verificarsi situazioni in cui risulta che le misure di controllo normalmente messe in atto sono inadeguate a gestire il rischio corruzione legato a una particolare attività, contratto o commessa e che non si vuole o non è possibile mettere in atto ulteriori misure di mitigazione.</p> <p>Se l'attività ad elevato rischio corruzione è già in atto, occorre interrompere o sospendere l'attività stessa appena possibile, nel frattempo devono essere messe in atto misure di controllo adeguate a contenere il rischio entro livelli accettabili. Questa situazione si può verificare al momento dell'avvio del sistema di gestione per prevenzione della corruzione, a seguito dell'analisi del rischio corruzione. Nel caso in cui l'attuazione dei controlli da parte del socio in affari richieda un certo tempo, l'organizzazione può proseguire la relazione con il socio in affari entro un tempo ragionevole, ma deve considerare tale circostanza nella propria valutazione dei rischi e applicare le eventuali misure compensative, quando necessarie (vedi A.13.3.7).</p> <p>Se la criticità viene individuata in relazione ad una attività (contratto, commessa) non ancora iniziata, occorre rinunciare all'attività stessa.</p>	<p>e dei contratti esistenti alla data di avvio del Sistema, comprese le informazioni raccolte in sede di due diligence, per le situazioni a rischio non trascurabile;</p> <ul style="list-style-type: none"> - registrazioni relative alla gestione di eventuali situazioni in cui si è riscontrata l'assenza o l'inadeguatezza dei controlli; - riesame della valutazione dei rischi e della capacità dell'organizzazione di contenere entro limiti accettabili i rischi connessi a queste situazioni; - decisioni assunte al riguardo in conformità alla politica e ai requisiti del sistema di gestione per la prevenzione della corruzione.
8.9 Segnalazione di sospetti	
<p>Devono essere attuate procedure che consentano di segnalare, "in buona fede e sulla base di una ragionevole convinzione":</p> <ul style="list-style-type: none"> - atti di corruzione, compiuti, tentati o presunti; - violazioni o carenze del sistema di gestione per la prevenzione della corruzione. <p>La norma prevede la possibilità di effettuare segnalazioni in forma anonima e, qualora il segnalante si identifichi, le segnalazioni devono essere trattate in modo confidenziale, al fine di proteggere l'identità del segnalante e di coloro che risultano coinvolti nella segnalazione, con il limite dettato dalle necessità di indagine o dalle richieste di Pubbliche Autorità.</p> <p>A tale proposito l'organizzazione dovrà applicare quanto previsto dalla legislazione vigente del Paese in cui lo standard è applicato e laddove non siano consentite segnalazioni in forma anonima e in via confidenziale, dovrà documentare (ad es. nella procedura delle segnalazioni) l'impossibilità di conformarsi al requisito, specificando i riferimenti di legge</p>	<p>Esempi di possibili evidenze per valutare la conformità al requisito possono essere:</p> <ul style="list-style-type: none"> - una procedura documentata per la gestione delle segnalazioni, con l'indicazione puntuale dei casi per i quali sono consentite le segnalazioni, modalità di trasmissione, trattamento dei dati inviati, destinatari, etc. - registrazioni circa la formazione erogata al personale sulla procedure di cui sopra, sulle tutele e sui diritti per i segnalanti, sulle conseguenze previste in caso di segnalazioni false o non veritiere; - previsione documentata del divieto di ritorsione; - organigrammi, job description o documenti equivalenti ove sono riportati flussi di comunicazione interna e compiti/responsabilità dei destinatari della segnalazioni, preposti al trattamento delle stesse; - contratti o incarichi (documentati) con sog-

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
<p>applicabili.</p> <p>Oltre alla funzione di conformità per la prevenzione della corruzione, l'organizzazione deve definire chi sono gli altri destinatari della segnalazione, ovvero i soggetti preposti ad analizzare la situazione e a prendere decisioni in merito all'eventuale avvio di indagini di approfondimento ai sensi del successivo p.to 8.10.</p> <p>Questi soggetti potrebbero essere individuati nell'ambito delle funzioni di controllo interno o tra gli organismi di vigilanza esterna dell'organizzazione (ad esempio, in Italia, l'Organismo di Vigilanza ai sensi del D. Lgs 231/2001).</p> <p>Il personale deve essere edotto sulle procedure di segnalazione e deve essere consapevole dei propri diritti e delle tutele riservate a coloro che effettuano segnalazioni nonché delle conseguenze previste in caso di segnalazioni false o non veritiere.</p> <p>In questo ambito rientra l'espressa previsione (ad esempio nella politica, nei contratti, nelle procedure) da parte dell'organizzazione del divieto di ritorsioni, e del corrispondente diritto a non subirne, per coloro che effettuano segnalazioni, nei termini previsti da questo requisito e dal p.to 7.2.2.2 della norma.</p> <p>L'organizzazione deve individuare e mettere a disposizione del personale un supporto qualificato (anche esterno) per fornire informazioni su come affrontare i sospetti casi di corruzione, in particolare per chiarire le fattispecie oggetto di segnalazione, le modalità di invio e trasmissione, le tutele riservate al segnalante, anche con riferimento all'eventuale avvio di indagini dirette ad acclarare i fatti.</p>	<p>getti esterni individuati come destinatari delle segnalazioni, preposti al trattamento delle stesse (quale, ad esempio, in Italia, l'Organismo di Vigilanza ai sensi del D. Lgs 231/2001);</p> <ul style="list-style-type: none"> - verifica dei canali utilizzati per le comunicazioni con questi soggetti esterni; - registrazioni (a campione) delle modalità di gestione delle segnalazioni pervenute, verifica da effettuarsi entro i limiti previsti dalla legge o concordati con il cliente circa la tutela dell'identità dei soggetti coinvolti e della riservatezza della informazioni contenute; - interviste con il personale per valutare il livello di sensibilità/consapevolezza circa le procedure di segnalazione. <p>Qualora vi siano disposizioni di legge per la disciplina delle segnalazioni o cd. "whistleblowing" (In Italia, la legge 179 del 30/11/2017) occorre verificare che l'organizzazione abbia identificati i relativi obblighi e li abbia integrati nelle proprie procedure.</p> <p>Questi obblighi potrebbero riguardare, ad esempio, le modalità di trasmissione della segnalazione: in via cartacea (es: cassetta presente presso il luoghi di lavoro) o elettronica (casella e-mail dedicata, sito web ecc...) ovvero della garanzia dell'anonimato della segnalazione in funzione dell'eventuale utilizzo nell'ambito di procedimenti disciplinari, indagini di polizia giudiziaria, etc.</p>
8.10 Indagini e gestione della corruzione	
<p>Qualora sia segnalato, rilevato o presunto un caso di corruzione o una violazione della politica di prevenzione della corruzione o del Sistema di Gestione (cfr. p.to 8.9), l'organizzazione deve avviare attività di indagine.</p> <p>L'organizzazione, come accennato al punto precedente, deve stabilire ruoli e responsabilità (anche all'esterno) per gestire la segnalazione, avviare e condurre l'indagine, per prendere decisioni all'esito delle indagini.</p> <p>La tipologie e le modalità di indagine variano in funzione delle dimensioni e delle caratteristiche dell'organizzazione e dell'entità dei fatti segnalati.</p>	<p>Esempi di possibili evidenze per valutare la conformità al requisito possono essere:</p> <ul style="list-style-type: none"> - una procedura o delle istruzioni per la gestione delle indagini, ove sono specificati i flussi di comunicazione, con l'indicazione dei compiti e delle responsabilità per l'avvio delle indagini, per la conduzione delle indagini, per la gestione dei risultati delle indagini, compreso il riesame delle procedure del sistema di gestione della prevenzione della corruzione; - contratti o incarichi (documentati) con soggetti individuati per la conduzione del-

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
<p>La funzione di conformità per la prevenzione della corruzione (cfr. p.to 5.3.2.) dovrebbe avere un ruolo centrale nel coordinamento delle indagini.</p> <p>Le indagini dovrebbero essere condotte da soggetti indipendenti ed imparziali rispetto all'oggetto di indagine (ad esempio, non appartenenti alla medesima funzione), oltre che muniti della necessaria competenza ed esperienza in relazione al caso da indagare.</p> <p>L'indagine potrebbe essere svolta da un soggetto terzo (quale ad esempio, in Italia, l'Organismo di Vigilanza ai sensi del D. Lgs 231/2001).</p> <p>L'organizzazione deve predisporre strumenti adeguati per assicurarne la riservatezza delle informazioni raccolte e sugli esiti delle indagini, nei limiti previsti dalla legislazione dello Stato (o degli Stati) presso cui lo standard viene applicato.</p> <p>Se per effetto dell'indagine i fatti, le violazioni o i sospetti segnalati dovessero essere confermati è necessario stabilire i destinatari e i flussi di comunicazione per la gestione del follow up.</p> <p>I risultati delle indagini devono essere portati a conoscenza dell'Alta Direzione che deve mettere in atto azioni appropriate.</p> <p>Al termine delle indagini le procedure di prevenzione della corruzione dovrebbero essere riesaminate per valutare eventuali inadeguatezze e, se necessario, apportare miglioramenti.</p>	<p>le indagini (quale, ad esempio, in Italia, l'Organismo di Vigilanza ai sensi del D.Lgs 231/2001);</p> <ul style="list-style-type: none"> - documenti e registrazioni (a campione) relative ad indagini svolte e alle azioni intraprese a seguito della conclusione delle indagini, compresa , ove pertinente, l'applicazione di sanzioni disciplinari; questa verifica da effettuarsi, ove possibile ed entro i limiti previsti dalla legge o concordati con il cliente circa la tutela dell'identità dei soggetti coinvolti e della riservatezza della informazioni relative all'indagine; - ove applicabile, evidenza del riesame delle procedure di prevenzione della corruzione a seguito dei risultati delle indagini.
9 VALUTAZIONE DELLE PRESTAZIONI	
9.1. Monitoraggio, misurazione, analisi e valutazione	
<p>Il requisito richiede all'organizzazione di determinare i processi che sono oggetto di monitoraggio, i ruoli e le responsabilità di coloro che li realizzano e la periodicità dello stesso.</p> <p>Particolare attenzione deve essere riposta nella analisi e valutazione dei risultati desunti dai monitoraggi, che debbono essere opportunamente conservati congiuntamente con i metodi utilizzati.</p> <p>L'obiettivo del monitoraggio è quello di raccogliere dati e informazioni in modo sistematico al fine di valutare le prestazioni per la prevenzione della corruzione e l'efficacia del sistema di gestione, mettendo in condizione l'organizzazione di rispondere a</p>	<p>Occorre verificare le informazioni documentate (procedure, piani di monitoraggio, registrazioni, etc.) che diano evidenza del processo di monitoraggio adottato dall'organizzazione, il quale deve necessariamente individuare cosa è necessario porre sotto monitoraggio, come effettuarlo, chi lo realizza, a chi vanno riportati i risultati e la periodicità con la quale va effettuato.</p> <p>Il "cosa" monitorare, dovrebbe definire il perimetro del monitoraggio, gli elementi del sistema dai quali ricavare dati e informazioni utili per valutarne l'efficacia.</p> <p>Tra gli esempi forniti dalla "Guida all'Utilizzo" si citano:</p>

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
<p>domande quali, ad esempio (vedi A.19):</p> <ul style="list-style-type: none"> - i rischi di corruzione sono sotto controllo? - i livelli di rischio sono migliorati o peggiorati? - i controlli sono efficaci? - le anomalie riscontrate nei controlli sono trattate in modo da impedirne il ripetersi? - gli obiettivi sono stati raggiunti? - il personale è sufficientemente coinvolto, al fine di consolidare la cultura della legalità nell'organizzazione? - le risorse messe a disposizione rappresentano esclusivamente un costo per l'organizzazione o si traducono in opportunità di miglioramento? <p>Attraverso il monitoraggio dell'efficacia del sistema e l'analisi dei suoi risultati sarà possibile per l'organizzazione comprendere, se e in che misura, l'adozione di questi strumenti e le risorse messe a disposizione per attuarli, rappresentino esclusivamente un costo o si traducano in opportunità di miglioramento.</p>	<ul style="list-style-type: none"> - efficacia dei controlli, rispetto ai quali l'organizzazione non dovrebbe limitarsi a verificarne l'effettuazione in base a quanto pianificato ma anche approfondire i risultati in termini di gravità, sistematicità, ripetitività, diffusione, impatti sui rischi delle eventuali anomalie riscontrate; - non conformità ai requisiti e "near misses", ossia quegli eventi rilevanti per il sistema di prevenzione della corruzione, che pur non avendo determinato effetti negativi (ad esempio, perché impediti da una circostanza fortuita), sono potenzialmente in grado di produrre danni; - eventuali scostamenti nella pianificazione degli audit, rispetto a quanto programmato; - efficace attribuzione delle responsabilità rispetto alle esigenze del sistema di gestione e dei controlli per la prevenzione della corruzione. <p>La definizione del "perimetro" del monitoraggio deve risultare coerente con il quadro dei rischi di corruzione dell'organizzazione, dando evidenza che le diverse aree esposte al rischio sono sistematicamente tenute sotto controllo.</p> <p>Il "come" monitorare, dovrebbe dare evidenza della metodologia scelta / utilizzata per la realizzazione dei diversi controlli previsti, che possono prevedere aree a campione o mirate. Anche in questo caso è necessario che i criteri scelti per il monitoraggio siano funzionali ad assicurare una adeguata copertura dei rischi di corruzione dell'organizzazione.</p> <p>Il "chi" realizza il monitoraggio presuppone che l'organizzazione abbia individuato il soggetto o la funzione responsabile della sua gestione.</p> <p>In termini generali, occorre distinguere tra il soggetto responsabile dell'attuazione del controllo anti corruzione, che, di norma, si identifica nel responsabile del processo/attività, da colui che è responsabile del monitoraggio sull'efficacia di controllo, il quale potrebbe essere un soggetto (o funzione) di livello superiore o terzo rispetto al processo in oggetto, anche esterno all'organizzazione. Possono anche esservi dei casi in cui le re-</p>

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
	<p>sponsabilità per il monitoraggio del sistema dei controllo per la prevenzione della corruzione sono stabilite dalla legge.</p> <p>Si pensi, ad esempio, al Responsabile Prevenzione Corruzione (e della Trasparenza), da nominarsi ai sensi della legge 190/2012, o all'organismo di vigilanza previsto dal D.lgs. 231/2001.</p> <p>In questi casi, l'organizzazione deve uniformare ed armonizzare le responsabilità per il monitoraggio del sistema di gestione UNI ISO 37001 con quelle previste ex lege, valutandone la possibile coincidenza, e assicurando l'operatività in modo coordinato tra tutti i soggetti coinvolti attraverso adeguati flussi di comunicazione.</p> <p>L'organizzazione deve dimostrare che i risultati dei monitoraggi sono oggetto di analisi e valutazione metodica e sistematica, utilizzandoli come possibili input di riesami e/o in generale di azioni di miglioramento.</p>
9.2. Audit interno	
<p>La norma oltre a specificare le motivazioni per l'effettuazione di audit interni (ad intervalli pianificati), esplicita modalità e requisiti da tenere in considerazione nella preparazione del programma di audit interni.</p> <p>Per la conduzione degli audit si fa sempre riferimento alla norma ISO 19011. Devono essere garantite imparzialità ed indipendenza dell'auditor rispetto al processo sottoposto ad audit.</p> <p>I risultati degli audit devono essere riferiti ai dirigenti di competenza, alla funzione conformità per la prevenzione della corruzione, all'Alta Direzione e, quando opportuno, all'Organo Direttivo.</p> <p>Lo scopo principale di un audit interno o di prima parte è la valutazione dell'efficacia del sistema di gestione all'interno dell'area/funzione esaminata.</p> <p>Questo controllo interno deve valutare se le procedure messe in atto dall'organizzazione, gli standard di riferimento e gli strumenti che utilizza nella quotidianità, siano idonei per implementare il sistema, e, nel tempo, possano centrare gli obiettivi prefissati dall'organizzazione.</p>	<p>La norma richiede all'organizzazione di stabilire, attuare e mantenere uno o più programmi di audit, definendone i criteri e il campo di applicazione, selezionando gli auditor ed assicurando, in generale, i requisiti di obiettività, imparzialità, competenza ed indipendenza.</p> <p>La pianificazione degli audit dovrà tenere conto necessariamente della valutazione dei rischi dell'organizzazione, campionando con maggior frequenza processi / funzioni a maggior rischio corruttivo.</p> <p>Il rispetto del requisito potrebbe essere valutato attraverso:</p> <ul style="list-style-type: none"> - la verifica del programma di audit; - l'esame dei rapporti di audit; - la verifica della competenza ed indipendenza degli auditor; - la verifica delle azioni messe in atto a seguito dei risultati degli audit; - l'analisi del riesame di direzione. <p>Nel caso l'organizzazione sia già dotata di un modello organizzativo ex D.lgs. 231/2001, sarà necessario considerare nella pianificazione degli audit interni, i controlli e la vigilanza dell'Organismo di Vigilanza e le comunicazio-</p>

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
	<p>ni relative agli ambiti di reato corrispondenti. Qualora sia presente una funzione di internal audit cui sono demandati i controlli sulla compliance anche in tema di anti corruzione, è necessario:</p> <ul style="list-style-type: none"> - stabilire quale obiettivo comune di audit la conformità ai requisiti dell'intero sistema ISO 37001; - formare adeguatamente e qualificare tutte le funzioni preposte all'audit, siano esse lo stesso internal audit, le funzioni di auditing HSEQ dei sistemi gestionali già in essere o soggetti esterni; - assicurare, i requisiti di obiettività, imparzialità, competenza ed indipendenza del team nei confronti delle funzioni auditate.
9.3. Riesame di direzione	
9.3.1. Riesame da parte dell'Alta Direzione	
<p>In considerazione dei compiti assegnati all'Alta Direzione e descritti al p.to 5.2.1, il riesame da parte di quest'ultima è un momento fondamentale per analizzare periodicamente l'adeguatezza e l'efficacia del sistema di gestione per la prevenzione della corruzione e determinare l'eventuale necessità di azioni, anche di modifica/integrazione del sistema stesso. La periodicità del riesame deve essere definita dall'organizzazione, ma si raccomanda che sia almeno annuale.</p> <p>Devono essere considerati come elementi in ingresso (un vero e proprio "ordine del giorno" obbligatorio) tutti gli aspetti previsti dalla norma: stato delle azioni derivanti da precedenti riesami, compresi quelli della funzione compliance anti corruzione (cfr. p.to 9.4); modifiche degli aspetti pertinenti del sistema di gestione per la prevenzione della corruzione; prestazioni del sistema (risultati del monitoraggio, degli audit, delle attività di indagine interna) e dei livelli di rischio di corruzione dell'organizzazione; efficacia delle azioni intraprese per mitigare i rischi, opportunità di miglioramento.</p> <p>Le prestazioni del sistema devono essere riesaminate con l'obiettivo di verificare il funzionamento del sistema stesso e la sua efficacia: i risultati degli audit interni e delle azioni di monitoraggio e misurazione, delle NC e AC e dei "near miss" (ove considerati), delle indagini, nonché delle valutazioni di efficacia</p>	<p>Occorre verificare se l'organizzazione abbia stabilito la periodicità del riesame in base a fattori quali: indice di frequenza delle modifiche nell'attività o nella struttura organizzativa, scelta di effettuare un riesame integrato o separato rispetto a quello relativo agli altri sistemi di gestione, grado di maturità del sistema, numero dei processi e delle loro interazioni, numero di aree identificate a rischio di corruzione di livello superiore al basso, risultati dei riesami precedenti, ecc.</p> <p>Con riferimento alle modifiche di aspetti pertinenti del sistema di gestione per la prevenzione della corruzione che devono essere considerati tra gli elementi in ingresso del riesame, vi sono, ad esempio: modifiche nel quadro legislativo di riferimento o nella situazione del mercato; modifiche nella struttura societaria, nell'organizzazione, nei ruoli, nelle attività (es. nuovi prodotti/servizi), nelle zone in cui opera l'Organizzazione, nelle relazioni con soci in affari e con le Pubbliche Amministrazioni.</p> <p>Tra gli elementi in ingresso del riesame devono essere riportate (e documentate) le informazioni relative all'eventuale coinvolgimento dell'organizzazione, o di suoi esponenti, in indagini o procedimenti per fatti di corruzione,</p>

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
<p>(della formazione, dei controlli e di tutte le azioni intraprese per affrontare i rischi, ecc.) possono fornire un quadro di dettaglio dello stato di attuazione del sistema di gestione per la prevenzione della corruzione e quindi permettere di stabilire ulteriori azioni necessarie.</p> <p>L'output del riesame è costituito dalle decisioni necessarie per:</p> <ul style="list-style-type: none"> - assicurare la conformità e l'efficacia del sistema di gestione, in base all'analisi degli elementi in ingresso; - trattare le modifiche del sistema in modo da rispettare la politica per la prevenzione della corruzione e non aggravare i rischi; - cogliere le opportunità per il miglioramento continuo. <p>L'Alta Direzione ha la responsabilità di presentare una sintesi dei risultati del riesame all'Organo Direttivo, ove presente, e conservare evidenze documentate dei propri riesami.</p>	<p>o analoghi, al fine di valutarne gli impatti sul sistema di gestione per la prevenzione della corruzione e prendere le occorrenti decisioni. Esempi di output del riesame possono essere le decisioni relative a:</p> <ul style="list-style-type: none"> - all'aggiornamento del contesto e della politica; - all'aggiornamento/integrazione dell'analisi dei rischi, - al sistema dei controlli; - alla formazione del personale; - alla gestione dei follow up di segnalazioni di atti di corruzione o di violazioni del sistema; - all'intensificazione di audit interni su processi specifici, ecc. <p>Nel caso sia presente l'Organo Direttivo, l'organizzazione dovrebbe fornire evidenza di aver trasmesso la documentazione pertinente al riesame e/o di aver predisposto una sintesi degli elementi principali dei risultati del riesame e di averne illustrato i contenuti in occasione delle riunioni dell'Organo Direttivo.</p> <p>Nel caso in cui abbia adottato un Modello organizzativo ex D.lgs. 231/2001, l'Organizzazione dovrebbe valutare anche l'opportunità di trasmettere i risultati del riesame, o alcune delle informazioni pertinenti, all'Organismo di Vigilanza.</p> <p>Le modalità per documentare il riesame dell'Alta Direzione non differiscono da quelle già previste per altri sistemi di gestione (ad es. in forma di verbale, con eventuali allegati).</p>
9.3.2. Riesame da parte dell'Organo Direttivo	
<p>L'effettuazione di un riesame non solo da parte dell'Alta Direzione, ma anche da parte dell'Organo Direttivo (se presente) è un elemento peculiare della norma UNI ISO 37001 che rispecchia la sua impostazione sulle responsabilità per la definizione e l'attuazione delle politiche e degli obiettivi in materia di prevenzione della corruzione.</p> <p>Il riesame è lo strumento che assicura il coinvolgimento nel sistema UNI ISO 37001 dell'organo che detiene la responsabilità definitiva sulle decisioni di governo e di amministrazione dell'organizzazione, e a cui fa capo l'Alta Direzione.</p> <p>Anche il riesame dell'Organo Direttivo, come quello</p>	<p>Attraverso il riesame, è possibile verificare se l'Organo Direttivo (ove presente), abbia provveduto:</p> <ul style="list-style-type: none"> - ad approvare o a confermare la politica per la prevenzione della corruzione dell'organizzazione; - a verificare lo stato di attuazione del sistema di gestione per la prevenzione della corruzione, per quanto di sua competenza in relazione al ruolo ed autorità; - per quanto di sua competenza in relazione al ruolo e autorità, a dare conto delle risorse stanziate ed assegnate, atte a garantire un

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
<p>dell'Alta Direzione, deve essere documentato al fine di fornire evidenza della sua effettuazione.</p>	<p>efficace funzionamento del sistema di gestione anticorruzione;</p> <ul style="list-style-type: none"> - a dare conto della sorveglianza sull'Alta Direzione per quanto attiene all'attuazione del sistema di gestione per la prevenzione della corruzione. <p>Anche i risultati prefissati e/o raggiunti, sedimentati come informazioni documentate nei diversi verbali di riunione dell'Organo Direttivo, potrebbero trovare un naturale riepilogo in tale riesame.</p> <p>Quali input di questo riesame, sono considerate tutte le informazioni pertinenti ricevute dall'Alta Direzione, dalla funzione di conformità per la prevenzione della corruzione e da qualunque altra informazione richiesta ed ottenuta.</p> <p>Infine, ove non presente l'Organo Direttivo, tali attività, ricadono nelle competenze dell'Alta Direzione (p.to 5.1.1).</p>

9.4. Riesame da parte della funzione di conformità per la prevenzione della corruzione

<p>La funzione di conformità per la prevenzione della corruzione deve riferire a intervalli pianificati e in occasioni ad hoc, circa l'adeguatezza e la corretta implementazione del sistema di gestione per la prevenzione della corruzione, ivi compresi i risultati delle indagini e degli audit.</p> <p>Tale relazione dovrà essere indirizzata agli organi di potere, all'Organo Direttivo (se presente) e all'Alta Direzione, o alla commissione competente dell'Organo Direttivo o dell'Alta Direzione.</p>	<p>Il rispetto del requisito potrebbe essere verificato attraverso evidenze attestanti:</p> <ul style="list-style-type: none"> - la pianificazione del riesame e le logiche di questa pianificazione, con diretto riferimento all'analisi dei rischi; - la verbalizzazione dei riesami; - il corretto flusso informativo delle risultanze emerse dal verbale di relazione all'Alta Direzione; - gli eventuali output e risultanze (decisioni, obiettivi, azioni di miglioramento etc.); - la corrispondenza delle attività di controllo e monitoraggio con quanto previsto all'interno dell'analisi dei rischi. <p>Il riesame da parte della funzione di conformità per la prevenzione della corruzione, potrebbe prendere in considerazione, a titolo esemplificativo e non esaustivo anche:</p> <ul style="list-style-type: none"> - la gestione del personale, con particolare riferimento a ruoli considerati sensibili (nuove assunzioni, rotazione come misura di prevenzione del rischio etc.) verificando l'assenza di motivi di incompatibilità e/o inconfiribilità di incarichi per particolari posizioni dirigenziali o in conflitto; - la formazione erogata in materia di preven-
--	---

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
	<p>zione della corruzione e i suoi esiti;</p> <ul style="list-style-type: none"> - il monitoraggio su tutte le misure adottate e previste sui processi sensibili così come definiti dall'Organizzazione sulla base della propria valutazione dei rischi; - risultanze degli Audit interni ed esterni; - risultanze di eventuali audit o controlli sul modello organizzativo ai sensi del D.lgs. 231/2001 (es. in caso di segnalazioni per tentativi di corruzioni e/o movimenti sospetti di denaro etc..) e la pianificazione delle attività mirate ad approfondire le criticità; - le attività di controllo nei confronti di soci in affari; - la gestione di eventuali segnalazioni ricevute (whistleblowing); - eventuali procedimenti disciplinari o contenziosi in essere; - la correttezza e la trasparenza dei flussi informativi con i vari organi di controllo, interni ed esterni interessati (es. Internal Audit, Organismo di Vigilanza, Responsabile Prevenzione Corruzione ex. 190/2012, Organismi Interni di Valutazione), in modo da evitare duplicazione di controlli sugli stessi processi sensibili, e di pianificare interventi mirati ed efficaci per prevenire fenomeni corruttivi. <p>Il riesame dovrebbe essere integrato, o quantomeno coordinato, con le attività di verifica periodica dell'efficacia dei Piani Triennali della Prevenzione della Corruzione (e della Trasparenza) ai sensi della L. 190/2012, i cui esiti sono registrati nella relazione trasmessa annualmente dal RPCT.</p> <p>Nel caso in cui l'organizzazione si avvalga del supporto di un soggetto esterno ("socio in affari") per l'esecuzione del riesame, occorre verificare il costante e corretto flusso delle informazioni alla funzione di compliance anti-corruzione.</p>
10 MIGLIORAMENTO	
10.1. Non conformità e azione correttiva	
<p>La non conformità rappresenta il mancato soddisfacimento di un requisito (ad es., l'omessa applicazione di un controllo o di una procedura del sistema di gestione).</p>	<p>Il rispetto del requisito potrebbe essere verificato attraverso:</p> <ul style="list-style-type: none"> - esame delle registrazioni relative alla gestione delle non conformità incluse analisi delle

DESCRIZIONE DEL REQUISITO E RELATIVE CONSIDERAZIONI	POSSIBILI EVIDENZE A SUPPORTO DELLA CONFORMITÀ
<p>La non conformità può essere rilevata (ma non solo) a seguito di:</p> <ul style="list-style-type: none"> - monitoraggi; - audit interni; - controlli e indagini da parte dell'organizzazione o di parti terze; - segnalazioni interne o da parte di stakeholder. <p>Quando viene rilevata una "non conformità" l'organizzazione deve:</p> <ul style="list-style-type: none"> - intervenire per contenere gli effetti negativi immediati dello scostamento (se presenti); - analizzare la causa; - pianificare e attuare azioni correttive idonee a impedirne il ripetersi. <p>L'organizzazione deve effettuare una valutazione dell'efficacia delle azioni correttive intraprese.</p> <p>L'"azione correttiva" non solo è espressione dell'attività di miglioramento continuo richiesta dalla norma, ma rappresenta anche strumento fondamentale per l'applicazione della prevenzione del rischio di corruzione attraverso l'eliminazione definitiva delle cause e degli effetti negativi di eventi che possono avere impatti negativi sull'organizzazione.</p>	<p>cause, correzioni ed azioni correttive;</p> <ul style="list-style-type: none"> - analisi del completamento degli interventi correttivi secondo quanto pianificato e della verifica sulla loro efficacia; - interviste con i responsabili dell'attuazione delle azioni correttive al fine di valutarne l'efficacia.
10.2. Miglioramento continuo	
<p>Il miglioramento continuo costituisce il processo ininterrotto all'interno del quale il sistema di gestione cresce e si sviluppa ogni volta che un'opportunità di miglioramento (in termini di idoneità, adeguatezza ed efficacia del sistema gestione anticorruzione) viene identificata.</p> <p>Il miglioramento si attua quindi attraverso un'analisi continua delle performance del sistema di gestione anticorruzione, utilizzando tutti gli input a disposizione (riesame della direzione, azioni correttive, opportunità per il miglioramento, esiti del monitoraggio e dei controlli) e mettendo in atto le necessarie azioni per aggiornare il sistema al fine di contribuire a garantirne l'integrità e di mantenerne l'efficacia.</p>	<p>Il rispetto del requisito potrebbe essere verificato attraverso:</p> <ul style="list-style-type: none"> - l'esame dei risultati dei riesami del sistema di gestione per la prevenzione della corruzione; - l'esame delle eventuali strategie e politiche per il miglioramento; - l'analisi delle modifiche al sistema di gestione apportate: motivi che hanno portato alla modifica, modalità di gestione della stessa e verifica dell'efficacia; - analisi degli indicatori sulle prestazioni dell'organizzazione in materia di prevenzione della corruzione; - stato dei livelli di rischio di corruzione identificati dall'organizzazione. <p>Il requisito costituisce in ultima istanza l'elemento portante di tutto il sistema di gestione, per questo motivo gli elementi da verificare si ritrovano in maniera "trasversale" anche in riferimento a tutti i punti della norma.</p>

Allegato 1

Tabella di correlazione PTPC/MOG 231/SISTEMI DI GESTIONE UNI ISO 37001

Requisito	PTPCT L. 190
SCOPO	Prevenzione reati «corruzione» + maladministration
ANALISI DEL CONTESTO	X
DEFINIZIONE E VALUTAZIONE DEI RISCHI (APPROCCIO PER PROCESSI)	X
LEADERSHIP E RESPONSABILITÀ	X (Organo di indirizzo, RPCT, Dirigenti, Referenti)
CONTROLLI	X MISURE GENERALI (trasversali sull'intera amministrazione) MISURE SPECIFICHE (che incidono su problemi specifici individuati tramite l'analisi del rischio)
SEGNALAZIONI (WHISTLEBLOWING)	X
FORMAZIONE	X
MONITORAGGIO	(“verifica dell'efficacia”)
AUDIT INTERNI	-----
RIESAME PERIODICO DELL'AD E MIGLIORAMENTO CONTINUO	(aggiornamento PTPC)
SISTEMA DISCIPLINARE SANZIONATORIO	X
VIGILANZA	X

MOG D.Lgs. 231	SISTEMA DI GESTIONE ISO 37001
Prevenzione reati ex artt. 24 e 25 del D.L.gs 231/2001 se commessi nell'interesse o a vantaggio dell'ente	Prevenzione della corruzione in applicazione di leggi vigenti o di altri impegni volontariamente assunti
X	X
X	X
X	X
X	X (da estendersi a organizzazioni controllate e «soci in affari» con livelli di rischio superiori al basso)
X	X
X	X
X	X
-----	X
(aggiornamento MOG a seguito di violazioni/cambiamenti)	X
X	X
X	-----

Allegato 2

Tabella integrazione requisiti UNI ISO 37001 VS UNI ISO 9001:2015

Requisito	ISO 37001	ISO 9001:2015
CONTESTO	4.1	4.1
ESIGENZE E ASPETTATIVE DELLE PARTI INTERESSATE	4.2	4.2
VALUTAZIONE DEL RISCHIO DI CORRUZIONE	4.5.1	6.1.1
ORGANO DIRETTIVO E ALTA DIREZIONE	5.1.1 5.1.2	5.1.1
POLITICA PER LA PREVENZIONE DELLA CORRUZIONE	5.2	5.2
RUOLI, RESPONSABILITA' E AUTORITA'	5.3.1	5.3
AZIONI PER AFFRONTARE RISCHI ED OPPORTUNITA'	6.1	6.1
OBIETTIVI	6.2	6.2
RISORSE	7.1	7.1
COMPETENZA	7.2	7.2
CONSAPEVOLEZZA E FORMAZIONE	7.3	7.3
COMUNICAZIONE	7.4	7.4
INFORMAZIONI DOCUMENTATE	7.5	7.5
PIANIFICAZIONE E CONTROLLO OPERATIVI	8.1	8.1
MONITORAGGIO, MISURAZIONE, ANALISI E VALUTAZIONE	9.1	9.1
AUDIT INTERNO	9.2	9.2
RIESAME DA PARTE DELL'ALTA DIREZIONE (E DELL'ORGANO DIRETTIVO)	9.3.1 9.3.2	9.3
NON CONFORMITA' E AZIONE CORRETTIVA	10.1	10.2
MIGLIORAMENTO CONTINUO	10.2	10.3

CONFORMA

Associazione Organismi Certificazione Ispezione Prova e Taratura, opera nel settore TIC (Testing, Inspection, Certification), ovvero nel settore della Valutazione della Conformità intesa come l'insieme delle attività, generalmente svolte in regime di accreditamento e/o su autorizzazione dei Ministeri competenti, in ambito volontario o cogente, di attività di certificazione di sistemi di gestione, prodotto, personale e servizi, ispezioni, marcatura CE e prove di laboratorio e taratura.

Costituita nel 2012 da alcune fra le più importanti Organizzazioni a livello nazionale ed internazionale nel settore della Valutazione della Conformità di parte terza indipendente, conta oggi 26 Soci.

UNI Ente Italiano di Normazione - che ha concesso il patrocinio a questa pubblicazione - è un'associazione privata senza scopo di lucro riconosciuta dallo Stato e dall'Unione Europea, che da quasi 100 anni elabora e pubblica norme tecniche volontarie (le "norme UNI") in tutti i settori industriali, commerciali e del terziario.

Sono soci UNI le imprese, i professionisti, le associazioni, gli enti pubblici, i centri di ricerca, gli istituti scolastici e accademici, le rappresentanze dei consumatori, dei lavoratori e ambientaliste, il terzo settore e le organizzazioni non governative: una grande piattaforma dove le risorse migliori del Paese, attraverso un'ampia partecipazione, trovano soluzioni a beneficio di tutti, quale sistema aperto di trasferimento di conoscenza e di diffusione di valori, per fare bene le cose ma anche per dare il buon esempio, con una forma di partecipazione dal basso per un nuovo modello democratico.

UNI è il garante di un patto di sicurezza e di stabilità che consente di realizzare la sintesi delle soluzioni per tutti, sulla base della pluralità dei problemi dei singoli.

L'obiettivo si raggiunge mettendo al centro le persone di UNI e di tutti i suoi stakeholder, la loro professionalità e il loro senso di appartenenza, in un'identità capace di stimolare e soddisfare le necessità della società, lungo tutto il processo della normazione: dall'innovazione all'applicazione, passando dall'elaborazione, la diffusione e la formazione.

Sono Soci di CONFORMA:

AFNOR Italia Srl
Aicq Sicev Srl
Apice Srl
Asacert Srl
Boreas Srl
Cersa Srl
Certiquality srl
Conteco Check Srl
CSI SpA
CSQA Certificazioni srl
Dekra Testing and Certification srl
DNV GL Business Assurance Italia srl
Eco Certificazioni SpA
Eurofins Modulo Uno srl
Eurofins Product Testing Italy Srl
ICIM SpA
ICMQ Spa
IGQ
IMQ SpA
Istituto Italiano dei Plastici srl
McJ Srl
No Gap Controls Srl
Rina Services SpA
SGS Italia SpA
TuV Nord Italia Srl
UL International Italia Srl

CONFORMIA
Associazione Organismi Certificazione Ispezione Prove Taratura

Piazzale R. Morandi 2, 20121 Milano - Telefono 02.77790409
info@associazioneconforma.eu - c.f. e p. iva 07671900962
www.associazioneconforma.eu