



# PG14

## PRESCRIZIONI PER LA CERTIFICAZIONE ABMS

### Stato Revisioni

Rev	Data	Oggetto modifica	Emissione	Approvazione
0	20/09/18	PRIMA EMISSIONE	 RGQ	 AU

revisione	data	emissione	approvazione	Pagina
0	20/09/2018	RGQ	AU	1 di 28

## INDICE

1. SCOPO.....	2
2. GENERALITA'.....	2
3. RIFERIMENTI .....	2
4. TERMINI E DEFINIZIONI.....	3
5. ELEMENTI SPECIFICI DELLO SCHEMA.....	6
6. TIPOLOGIE DI SOGGETTI CHE POSSONO RICHIEDERE LA CERTIFICAZIONE E POSSIBILI ESCLUSIONI.....	7
7. METODOLOGIE DI VALUTAZIONE E PRESCRIZIONI RELATIVE ALL'AUDIT .....	7
7.1 Evidenze di audit .....	8
7.2 Prescrizioni relative agli audit.....	8
7.3 Scopo del certificato .....	9
8. BUONE PRATICHE NELLA GESTIONE DELLA PREVENZIONE DELLA CORRUZIONE.....	10

### 1. SCOPO

Scopo della presente procedura è definire le modalità operative e specifiche regole applicative per la certificazione di conformità alla ISO 37001:2016.

### 2. GENERALITA'

La ISO 37001 specifica le misure e i controlli adottabili da un'organizzazione per monitorare le proprie attività aziendali al fine di prevenire la corruzione. Rientrano tra questi la predisposizione di una politica anticorruzione, l'impegno in tal senso da parte dell'Alta Direzione, l'individuazione di un incaricato, la formazione continua di tutti gli interessati volta all'accrescimento della cultura organizzativa, la valutazione dei rischi specifici, la definizione di relative procedure, come ad esempio la regolamentazione di omaggi e regali, il monitoraggio dei fornitori e dei partner commerciali.

La società richiedente, per ottenere e mantenere la certificazione del proprio sistema di gestione per la prevenzione della corruzione, deve soddisfare i requisiti riportati nella norma di riferimento, nel presente regolamento, nella PG01 "Regolamento per la certificazione dei sistemi di gestione" e nelle condizioni generali di vendita, mantenendo successivamente il proprio Sistema di Gestione Aziendale in soddisfacente operatività.

### 3. RIFERIMENTI

- UNI ISO 37001:2016
- Manuale Qualità di GSC Global System Certification
- UNI CEI EN ISO/IEC 17021-1:2015
- Circolare Tecnica ACCREDIA CT N°28/2017
- REG 01-01 ACCREDIA

<i>revisione</i>	<i>data</i>	<i>emissione</i>	<i>approvazione</i>	<i>Pagina</i>
0	20/09/2018	RGQ	AU	2 di 28

#### 4. TERMINI E DEFINIZIONI

**Corruzione:** Offrire, promettere, fornire, accettare o richiedere un vantaggio indebito di qualsivoglia valore (che può essere economico o non economico), direttamente o indirettamente, e indipendentemente dal luogo, violando la legge vigente, come incentivo o ricompensa per una persona ad agire o a omettere azioni in relazione alla prestazione delle mansioni di quella persona.

*Nota: La definizione è da ritenersi generica. Il significato del termine "corruzione" è definito dalla legge anti-corruzione applicabile all'organizzazione e dal Sistema di gestione per la prevenzione della corruzione progettato dall'organizzazione.*

**Organizzazione:** Persona o gruppo di persone avente funzioni proprie con responsabilità, autorità e relazioni per conseguire i propri obiettivi.

*Note:*

*Il concetto di organizzazione comprende, in termini non esaustivi, singoli operatori, società, gruppi, aziende, imprese, autorità, partnership, enti di beneficenza o istituzioni, o loro parti o combinazioni, costituiti in persona giuridica o meno, pubblici o privati.*

*Nelle organizzazioni con più unità operative, una o più unità operative possono essere definite come un'organizzazione.*

**Parte interessata (termine preferito); stakeholder (termine ammesso):** Persona oppure organizzazione che può influenzare, essere influenzata, o percepire se stessa come influenzata da una decisione o attività.

*Nota: Gli stakeholder possono essere interni o esterni all'organizzazione.*

**Requisito:** Esigenza che è esplicita e obbligatoria.

*Note:*

*La definizione base di "requisito" nelle norme ISO sui sistemi di gestione è "esigenza o aspettativa che può essere esplicita, generalmente implicita oppure obbligatoria". I "requisiti generalmente impliciti" non sono applicabili nel contesto della gestione per la prevenzione della corruzione.*

*"Generalmente implicita" significa che è uso o prassi comune, per l'organizzazione e per le parti interessate, che l'esigenza o l'aspettativa in esame sia implicita.*

*Un requisito specificato è un requisito che è esplicitato, per esempio, in informazioni documentate.*

**Sistema di gestione:** Insieme di elementi correlati o interagenti di un'organizzazione finalizzato a stabilire politiche, obiettivi e processi per conseguire tali obiettivi.

*Note:*

*Un sistema di gestione può affrontare a una o più discipline.*

*Gli elementi del sistema comprendono la struttura, i ruoli e le responsabilità, la pianificazione e il funzionamento dell'organizzazione.*

*Il campo di applicazione di un sistema di gestione può comprendere l'intera organizzazione, funzioni specifiche e identificate dell'organizzazione, settori specifici e identificati dell'organizzazione, oppure una o più funzioni nell'ambito di un gruppo di organizzazioni.*

**Alta direzione:** Persona o gruppo di persone che, al livello più elevato, dirigono e controllano un'organizzazione.

*Note:*

*L'alta direzione ha il potere di delegare l'autorità e mettere a disposizione le risorse all'interno dell'organizzazione.*

*Se il campo di applicazione del sistema di gestione copre solo parte di un'organizzazione, il termine alta direzione si riferisce a coloro che dirigono e controllano quella parte dell'organizzazione.*

*Le organizzazioni possono essere organizzate in base al quadro normativo secondo cui sono obbligate a operare e anche secondo le loro dimensioni, il loro settore, ecc. Alcune organizzazioni hanno sia un organo direttivo sia un'alta direzione, mentre alcune organizzazioni non ripartiscono le responsabilità fra diversi organi. Tali variazioni, sia in rispetto dell'organizzazione sia delle responsabilità, possono essere tenute in considerazione durante l'applicazione dei requisiti relativi alla leadership.*

revisione	data	emissione	approvazione	Pagina
0	20/09/2018	RGQ	AU	3 di 28

**Organo direttivo:** Gruppo o organo che detiene la responsabilità definitiva e l'autorità per le attività, l'amministrazione e le politiche dell'organizzazione a cui fa capo l'alta direzione e che controlla le responsabilità dell'alta direzione.

*Note:*

*Non tutte le organizzazioni, soprattutto quelle piccole, possiedono un organo direttivo separato dall'alta direzione.*

*Un organo direttivo può includere, a titolo non esaustivo, il consiglio direttivo, le commissioni del consiglio direttivo, il consiglio di sorveglianza, i membri del consiglio di amministrazione ed i supervisori.*

*Funzione di conformità per la prevenzione della corruzione: La persona o le persone aventi la responsabilità e l'autorità per il funzionamento del sistema di gestione per la prevenzione della corruzione.*

**Efficacia:** Grado di realizzazione delle attività pianificate e di conseguimento dei risultati pianificati.

**Politica:** Orientamenti e indirizzi di un'organizzazione espressi in modo formale dalla propria alta direzione o dal proprio organo direttivo.

**Obiettivo:** Risultato da conseguire.

*Note:*

*Un obiettivo può essere strategico, tattico od operativo.*

*Gli obiettivi possono riguardare differenti discipline (quali obiettivi finanziari, per vendita e marketing, per l'approvvigionamento, per salute e sicurezza e ambientali) e possono applicarsi a livelli differenti, come quello strategico, dell'intera organizzazione, di progetto, di prodotto e di processo.*

*Un obiettivo può essere espresso in altri modi, per esempio come un esito previsto, uno scopo, un criterio operativo, come un obiettivo per la prevenzione della corruzione, oppure mediante l'utilizzo di altre parole di significato simile (per esempio fine, scopo o traguardo).*

*Nel contesto dei sistemi di gestione per la prevenzione della corruzione, gli obiettivi per la prevenzione della corruzione sono definiti dall'organizzazione, coerentemente alla politica di prevenzione della corruzione per conseguire risultati specifici.*

**Rischio:** Effetto dell'incertezza sugli obiettivi.

*Note:*

*Un effetto è uno scostamento da quanto atteso - positivo o negativo.*

*Incertezza è lo stato, anche parziale, di carenza di informazioni relative alla comprensione o conoscenza di un evento, delle sue conseguenze o della sua probabilità.*

*Il rischio è spesso caratterizzato dal riferimento a potenziali "eventi" e "conseguenze", o da una loro combinazione.*

*Il rischio è spesso espresso in termini di combinazione delle conseguenze di un evento e della "probabilità" associata al suo verificarsi (cfr. Guida ISO 73:2009).*

**Competenza:** Capacità di applicare conoscenze e abilità per conseguire i risultati attesi.

**Informazioni documentate:** Informazioni che devono essere controllate e conservate da parte di un'organizzazione incluso il supporto che le contiene.

*Note:*

*Le informazioni documentate possono essere in qualsiasi formato, su qualsiasi supporto e provenire da qualsiasi fonte.*

*Le informazioni documentate possono riferirsi a: il sistema di gestione, compresi i relativi processi; le informazioni prodotte per il funzionamento dell'organizzazione (documentazione); l'evidenza dei risultati conseguiti (registrazioni).*

**Processo:** Insieme di attività correlate o interagenti che trasformano input in output.

**Prestazioni:** Risultati misurabili.

*Note:*

*Le prestazioni possono riguardare risultanze sia quantitative sia qualitative.*

revisione	data	emissione	approvazione	Pagina
0	20/09/2018	RGQ	AU	4 di 28

*Le prestazioni possono riguardare la gestione di attività, processi, prodotti (compresi i servizi), sistemi oppure organizzazioni.*

**Affidare all'esterno, esternalizzare** (verbo): Stipulare un accordo nel quale un'organizzazione esterna esegue parte di una funzione o di un processo dell'organizzazione.

*Nota:*

*Un'organizzazione esterna è fuori dal campo di applicazione del sistema di gestione, anche se la funzione o il processo affidato all'esterno ricade nel campo di applicazione stesso.*

*Il testo base delle norme ISO sui sistemi di gestione contiene una definizione e un requisito relativamente all'affidamento all'esterno (outsourcing), che non sono utilizzati nel presente documento, in quanto i fornitori esterni rientrano nella definizione di soci in affari.*

**Monitoraggio:** Determinazione dello stato di un sistema, di un processo o di un'attività.

*Nota:*

*Per determinare lo stato può essere necessario verificare, sorvegliare oppure osservare in modo critico.*

**Misurazione:** Processo per determinare un valore.

**Audit:** Processo sistematico, indipendente e documentato per ottenere evidenze dell'audit e valutarle oggettivamente al fine di determinare in quale misura i criteri dell'audit siano stati soddisfatti.

*Nota:*

*Un audit può essere un audit interno (di prima parte) o un audit esterno (di seconda parte o di terza parte) e può essere un audit combinato (che combina due o più discipline).*

*Un audit interno è condotto dall'organizzazione stessa o da una parte esterna per suo conto. Le "evidenze dell'audit" e i "criteri dell'audit" sono definiti nella ISO 19011.*

**Conformità:** Soddisfacimento di un requisito.

**Non conformità:** Mancato soddisfacimento di un requisito.

**Azione correttiva:** Azione tesa a eliminare la causa di una non conformità e a impedirne la ricorrenza.

**Miglioramento continuo:** Attività ricorrente di miglioramento della prestazione.

**Personale:** Dirigenti, funzionari, dipendenti, staff o lavoratori temporanei e volontari dell'organizzazione.

*Nota:*

*Tipologie diverse di personale pongono tipologie e gradi diversi di rischio di corruzione e possono essere trattate in modo differenziato dalle procedure di valutazione del rischio di corruzione e di gestione del rischio di corruzione dell'organizzazione.*

*Per una guida sullo staff ed i lavoratori temporanei cfr. §8.8*

**Socio in affari:** Parte esterna con cui l'organizzazione ha o progetta di stabilire una qualsivoglia forma di relazione commerciale.

*Nota:*

*I soci in affari comprendono, a titolo non esaustivo, clienti, acquirenti, "joint venture", partner in joint venture, partner in consorzio, fornitori esterni, appaltatori, consulenti, sub-appaltatori, fornitori, venditori, esperti, agenti, distributori, rappresentanti, intermediari e investitori. La presente definizione è appositamente ampia e dovrebbe essere interpretata in linea con il profilo del rischio di corruzione dell'organizzazione da applicare ai soci in affari che possono ragionevolmente esporre l'organizzazione ai rischi di corruzione.*

*Tipologie diverse di soci in affari pongono tipologie e gradi diversi di rischio di corruzione e un'organizzazione ha diversi gradi di abilità di influenzare tipologie diverse di soci in affari. Tipologie diverse di soci in affari possono essere trattate in modo differenziato dalle procedure di valutazione del rischio di corruzione e di gestione del rischio di corruzione dell'organizzazione.*

*L'espressione "affari" nella presente norma internazionale può essere intesa in senso ampio, indicando quelle attività che sono pertinenti agli scopi dell'organizzazione.*

revisione	data	emissione	approvazione	Pagina
0	20/09/2018	RGQ	AU	5 di 28

**Pubblico ufficiale:** Persona che ricopre incarichi legislativi, amministrativi o giudiziari, indipendentemente che derivino da nomina, elezione o successione, o qualsiasi persona che eserciti una funzione pubblica, incluse quelle per un'agenzia pubblica o un'impresa pubblica, oppure qualsiasi funzionario o agente di un'organizzazione pubblica, nazionale o internazionale, o qualsiasi candidato per un incarico pubblico.

*Nota:*

*Per gli esempi di individui che possono essere considerati pubblici ufficiali, cfr. §8.21*

**Parte terza:** Persona o ente indipendente dall'organizzazione.

*Nota:*

*Tutti i soci in affari sono parti terze, ma non tutte le parti terze sono soci in affari.*

**Conflitto di interessi:** Situazione in cui gli interessi commerciali, economici, famigliari, politici o personali potrebbero interferire con il giudizio degli individui nello svolgimento delle loro funzioni per l'organizzazione.

**Due diligence:** Processo per valutare ulteriormente la natura e l'entità del rischio di corruzione e aiutare le organizzazioni ad assumere decisioni in relazione a transazioni, progetti, attività, soci in affari e personale specifici.

Per la terminologia e le definizioni non espressamente evidenziate, si rimanda alle ISO 37001, ISO/IEC 17000, ISO/IEC 17021, Manuale Qualità GSC Global System Certification.

## 5. ELEMENTI SPECIFICI DELLO SCHEMA

Il significato di "corruzione" cui fa riferimento la norma ISO 37001 comprende tutte le condotte o attività che, ancorché formalmente lecite, sono rilevanti (direttamente o indirettamente) sotto il profilo dei rischi di corruzione e si pongono come ostacolo rispetto al perseguimento delle finalità d'interesse generale cui sono preposte sia le organizzazioni pubbliche che quelle private (si vedano ad es. le organizzazioni non profit, di cooperazione sociale, della sanità e dell'istruzione private, le imprese private appaltatrici di pubblici servizi, le organizzazioni non governative, ecc.).

La verifica circa la corretta implementazione dei requisiti posti dallo standard deve essere focalizzata sul controllo della corretta definizione ed applicazione delle procedure predisposte dall'organizzazione al fine di gestire i cosiddetti processi critici, così come emersi dall'analisi dei rischi e dalle eventuali due diligence, secondo quanto previsto dalla norma stessa. La descrizione formale delle attività sensibili è il primo passo per effettuare attività di controllo tramite audit. Si sottolinea che, ai fini del presente documento, si ritengono sensibili dal punto di vista della corruzione tutti i processi/funzioni identificati dall'organizzazione come a maggior rischio di corruzione, oltre a tutti quelli "sensibili" espressamente richiamati nel documento Accredia CT n.28/2017<sup>1</sup>.

Un elemento essenziale nel processo di certificazione è rappresentato dalle informazioni che l'organizzazione cliente fornisce all'organismo di certificazione. Infatti, l'audit di prima certificazione avviene in organizzazioni delle quali l'organismo non ha dati ex ante, se non quelli ricavati dalla dichiarazione spontanea della stessa organizzazione, o per notizie apprese dai media. Questo aspetto è particolarmente critico, dal momento che non è sempre possibile comprendere se l'impresa, pur munita di corrette procedure (adottate o meno in applicazione alla legislazione applicabile in tema di corporate crime), rappresenti un "ambiente patologico" sotto il profilo della corruzione. Lo standard ha infatti finalità preventiva, che risulta incompatibile con un ambiente di impresa patologico, che necessita di correzione anziché di prevenzione.

Si osservi che qualsiasi ambiente contaminato da pratiche corruttive, con le connessioni criminali che spesso le accompagnano, anche se mai toccato da indagini di polizia giudiziaria, sarà comunque un contesto ove lo sviluppo ed efficace applicazione del sistema di gestione non può avere un approccio preventivo, ma correttivo, e sarà anche osteggiato, più probabilmente pilotato, proprio da quella compagine che ha interesse a creare una immagine di apparente legalità, funzionale alla perpetrazione delle pratiche di corruzione.

<sup>1</sup> Elenco non esaustivo di attività e processi sensibili: finanza e controllo, commerciale, agenti e rete vendita, approvvigionamento, figure istituzionali e organi sociali, Uffici di direzione e CdA, internal auditing, gestione licenze, gare e autorizzazioni, gestione risorse umane (compreso gestione, selezione, assunzioni e avanzamenti di carriera), amministrazione e gestione cassa, acquisti, gestione omaggi e liberalità, relazioni con autorità istituzionali ed enti di controllo, gestione patrocini e sponsor, gestione contenziosi e reclami, servizi informatici, gestione security, attività di controllo e collaudi.

revisione	data	emissione	approvazione	Pagina
0	20/09/2018	RGQ	AU	6 di 28

Diversamente, un'azienda che dichiara spontaneamente un'eventuale esistenza di situazioni "critiche" o già rilevanti a livello giudiziario, può essere ritenuta idonea per il percorso di certificazione, con approccio correttivo, ma anche di sviluppo di prassi preventive. Infatti, in questo secondo caso, l'adozione del sistema di gestione anticorruzione sarà da intendersi come azione ampia e strutturata a livello sistemico, finalizzata e coerente con un approccio terapeutico aziendale che dovrà risultare fortemente sponsorizzato dalla direzione.

La cultura di compliance deve essere pervasiva di tutta l'organizzazione. Il sistema di gestione anticorruzione deve essere applicato a tutti i processi aziendali, al fine di scongiurare il rischio di permanenza di situazioni scarsamente trasparenti che possono rendere vana l'applicazione dell'intero sistema di gestione. La visione globale nell'applicazione del sistema di gestione deve coinvolgere tutti i processi organizzativi e in outsourcing almeno in fase di analisi preliminare di contesto e, solo dopo tale valutazione, possono essere enucleati, con adeguate argomentazioni, i processi considerati non critici, per i quali la valutazione dei rischi potrà limitarsi a questo primo livello di approfondimento.

Sarà dunque necessario interpretare e relativizzare a seconda del caso concreto quanto indicato al § A.4.1., relativo alla valutazione dei rischi.

La metodologia suesposta deve essere rigorosamente applicata al fine di evitare l'insorgenza di situazioni opinabili e per le quali la certificazione potrebbe avere delle aree di debolezza strutturale di credibilità; il tempo da allocare a tale verifica di conseguenza dovrà essere sufficiente a comprendere se ci si trovi di fronte a un sistema di gestione efficacemente applicato.

Laddove il GA venisse a conoscenza, direttamente dall'organizzazione o da altre fonti, che la stessa organizzazione è implicata con dei profili di responsabilità in scandali o procedimenti giudiziari per fenomeni corruttivi, dovrà darne immediata comunicazione al Direttore di GSC-Global System Certification, il quale provvederà a predisporre la tempestiva valutazione degli specifici eventi ed i consueti provvedimenti del caso (per esempio chiusura della valutazione con archiviazione, adozione dei provvedimenti previsti dai regolamenti di certificazione, rafforzamento della attività ispettive), definiti in funzione della adeguatezza della risposta e delle strategie adottate dall'organizzazione.

## 6. TIPOLOGIE DI SOGGETTI CHE POSSONO RICHIEDERE LA CERTIFICAZIONE E POSSIBILI ESCLUSIONI

La certificazione ISO 37001 può essere richiesta da qualunque tipo di organizzazione, di qualsiasi dimensione o natura.

La certificazione viene rilasciata ad una sola entità giuridica e comprende tutti i siti, filiali, sedi secondarie, attività e processi effettivamente svolti dall'organizzazione.

Non sono ammesse esclusioni a processi/funzioni svolte in una stessa Nazione.

È possibile limitare l'applicazione a specifiche Nazioni, ma il campo di applicazione deve sempre includere processi e attività sensibili sviluppati all'estero quando svolti sotto la responsabilità e il diretto controllo dell'organizzazione (es. uffici di rappresentanza o sedi secondarie agenti o mediatori): questo aspetto deve essere ben esplicitato nei report di audit.

Nel caso di gruppi di società, quando attività/processi sensibili siano svolti da altre società del gruppo (capogruppo e/o controllate), anche all'estero, si applicano le prescrizioni relative alla "Attuazione dei controlli per la prevenzione della corruzione da parte di organizzazioni controllate e soci in affari" (cfr. UNI ISO 37001 §8.5).

Il GA dovrà tener presente che la conformità ai requisiti di modelli e sistemi di prevenzione previsti da norme di legge (es. Modelli Organizzativi ai sensi del D.Lgs. 231/2001, PTPC ai sensi della L. 190/2012 e simili) non è certificabile.

## 7. METODOLOGIE DI VALUTAZIONE E PRESCRIZIONI RELATIVE ALL'AUDIT

Lo standard UNI ISO 37001 richiede l'adozione di alcuni elementi portanti, tra cui:

- una politica per la prevenzione della corruzione, procedure e controlli;
- comunicazione di tale politica e del relativo programma a tutte le parti interessate e/o associate;
- la leadership, l'impegno e la responsabilità;
- una procedura di sorveglianza;
- formazione relativa alla prevenzione della corruzione;

<i>revisione</i>	<i>data</i>	<i>emissione</i>	<i>approvazione</i>	<i>Pagina</i>
0	20/09/2018	RGQ	AU	7 di 28

- effettuazione della valutazione dei rischi su tutti i processi/attività;
- due diligence su progetti e business partner dell'organizzazione;
- reporting, monitoraggio, indagine e riesame dell'Alta Direzione e, se presente, dell'Organo di governance;
- richiesta di sottoscrivere un impegno per la prevenzione della corruzione ai propri associati;
- implementare i controlli finanziari a ridurre i rischi di corruzione;
- azioni correttive e di miglioramento continuo.

Si precisa che, con riferimento all'analisi dei rischi corruzione elaborata dall'organizzazione, il GA non potrà limitarsi a prendere atto dell'esistenza del documento; sarà necessario partire dalla definizione che l'organizzazione si è data di corruzione che, si rammenta, non può essere meno restrittiva di quella prevista per legge. Tale definizione deve essere coerente con l'analisi di contesto effettuata. Il GA dovrà valutare la completezza ed esaustività dell'analisi dei rischi di corruzione, con riferimento ai requisiti applicabili della norma, e la robustezza del processo di internal auditing per la fattispecie della corruzione, che dovrà essere basato (pianificazione, programmazione ed esecuzione) sui risultati della valutazione dei rischi e della mitigazione adottata, sulle valutazioni di rischio residuo e sul testing dei controlli operativi.

Il GA dovrà valutare con maggiore frequenza, impegno e profondità i processi/funzioni identificati dall'organizzazione e/o dallo stesso GA come a maggior rischio, riportandone una spiegazione nella documentazione di verifica, oltre a quelli "sensibili" espressamente richiamati nel documento Accredia CT n.28/2017.

Al fine di preservare l'efficacia delle attività di audit, si raccomanda di dedicare tempi adeguati all'effettuazione di interviste, verifiche puntuali su transazioni, relazioni con business partner, processi a rischio, analisi delle notizie di pubblico dominio rilevanti, test sulla diffusione dei sistemi di controllo interno. Si raccomanda inoltre di stabilire metodiche in grado di assicurare campionamenti rappresentativi in funzione dei rischi, di dedicare tempi adeguati non a controlli "in astratto" e sulla "carta" ma effettuando interviste, verifiche puntuali su transazioni, relazioni con business partner, processi a rischio, analisi delle notizie di pubblico dominio rilevanti, test sulla diffusione dei sistemi di controllo interno.

## 7.1 Evidenze di audit

Particolare attenzione dovrà essere posta nella valutazione e registrazione di evidenze relative a:

- perimetro ed applicabilità del Sistema di Gestione (4.3 della ISO 37001);
- definizione di corruzione prevista per l'organizzazione, sviluppata sulla base dell'analisi di contesto;
- specifici dettagli in merito alle attività a rischio, riportando in dettaglio processi a rischio ed attività sensibili;
- mappatura dei soggetti interni ed esterni che sono coinvolti in attività a maggior rischio;
- indicazione dei Partner in Affari e tipo di monitoraggio sugli stessi (tipo di gestione da questi adottata in ottica anticorruzione);
- eventuali relazioni societarie;
- riferimenti legislativi specifici;
- specifiche indicazioni sulla formazione svolta;
- elenco delle commesse valutate;
- analisi degli eventuali episodi di corruzione verificatisi e le contromisure adottate.

## 7.2 Prescrizioni relative agli audit

Con riferimento all'iter di certificazione si ritengono applicabili tutte le prescrizioni generali previste nella ISO77"Audit in campo" e nella PG01"Regolamento di certificazione dei sistemi di gestione", con le precisazioni appresso descritte.

Per quanto attiene la valutazione degli addetti equivalenti, è necessario considerare la totalità degli addetti coinvolti in attività e processi sensibili (cfr. nota 1 §5). È possibile effettuare un adeguamento mediante radice quadrata per gli addetti equivalenti impiegati nei processi operativi di produzione o di erogazione dei servizi, solo nel caso in cui questi processi presentino bassi rischi di corruzione sulla base della valutazione dei rischi effettuata dall'organizzazione, e comunque sempre con esclusione degli addetti coinvolti nei

<i>revisione</i>	<i>data</i>	<i>emissione</i>	<i>approvazione</i>	<i>Pagina</i>
0	20/09/2018	RGQ	AU	8 di 28

processi/attività sensibili. Parimenti, nel caso in cui processi/attività sensibili dell'organizzazione siano svolti in outsourcing (ad es. consorzi), il calcolo degli addetti deve tenere conto anche di tali soggetti.

Nel corso dell'audit di stage 1, il GA deve riesaminare, in funzione dei rischi di corruzione identificati, la ragionevolezza dell'eventuale adeguamento applicato in fase di emissione dell'offerta di certificazione e deve verificare la congruenza del numero di addetti comunicati dall'organizzazione in sede di definizione del contratto. Questa valutazione deve essere registrata sui rapporti di audit.

Lo Stage 1 deve essere effettuato sempre c/o l'Organizzazione anche nel caso di realtà di piccole dimensioni ed ha durata minima mai inferiore a 1.00 g/u.

Per i Multisito, si applicano i documenti IAF in vigore.

Non possono essere esclusi dalla base del campionamento siti ove vengono svolti processi/attività a rischio corruzione (si veda la nota 1 e l'analisi rischi predisposta dall'organizzazione).

### 7.3 Scopo del certificato

I criteri per la formulazione dello scopo del certificato sono gli stessi applicabili per la ISO 9001, con particolare attenzione alle attività svolte.

Deve essere chiarito nel campo di applicazione se l'organizzazione detiene il controllo su altre organizzazioni, specificando le caratteristiche di tale controllo (es. partecipazioni al capitale, vincoli contrattuali, etc.).

<i>revisione</i>	<i>data</i>	<i>emissione</i>	<i>approvazione</i>	<i>Pagina</i>
0	20/09/2018	RGQ	AU	9 di 28

## 8. BUONE PRATICHE NELLA GESTIONE DELLA PREVENZIONE DELLA CORRUZIONE

### 8.1 Generalità

In questo paragrafo è fornita un'interpretazione dei requisiti applicabili ai Sistemi di Gestione per la prevenzione della corruzione, unitamente ad indicazioni concrete sulla corretta applicazione degli stessi requisiti e uno strumento per la valutazione della conformità e dell'efficacia di un Sistema di Gestione.

Il presente documento è da ritenersi esemplificativo e non intende essere esaustivo. Ai fini della conformità del sistema di gestione per la prevenzione della corruzione ai requisiti della UNI ISO 37001, è necessario che le misure adottate dall'organizzazione siano ragionevoli e proporzionate alla natura e all'entità dei rischi di corruzione a cui la stessa organizzazione è sottoposta (si vedano il punto 4.5 e i fattori di cui ai punti 4.1 e 4.2 della norma).

### 8.2 Campo di applicazione del sistema per la prevenzione della corruzione

#### 8.2.1 Sistema di gestione per la prevenzione della corruzione a sé stante o integrato

Il sistema di gestione per la prevenzione della corruzione può essere adottato come sistema separato o come parte integrante di un sistema di gestione di conformità complessivo. L'organizzazione può anche scegliere di adottare il sistema di gestione per la prevenzione della corruzione in parallelo ai propri altri sistemi di gestione, oppure come parte di essi, come il sistema di gestione qualità, quello sulla sicurezza ambientale e quello sulla sicurezza delle informazioni.

#### 8.2.2 Pagamenti agevolativi ed estorti

**8.2.2.1** Per pagamento agevolativo si intende il termine che talvolta si dà a un pagamento illecito o non ufficiale effettuato in cambio di servizi che il pagatore è legalmente legittimato a ottenere senza eseguire tale pagamento. Normalmente si tratta di un pagamento di entità relativamente bassa fatto a un pubblico ufficiale o a una persona con funzione di certificatore al fine di assicurarsi o velocizzare la prestazione di un intervento di routine o necessario, come l'emissione di un visto, di un permesso di soggiorno, lo sdoganamento o l'installazione di una linea telefonica. Sebbene la natura dei pagamenti agevolativi sia spesso ritenuta differente rispetto a, per esempio, una tangente pagata per fare affari, essi sono illeciti in molti luoghi e sono considerati tangenti ai fini del presente documento e dovrebbero essere vietati dal sistema di gestione per la prevenzione della corruzione dell'organizzazione.

**8.2.2.2** Un pagamento estorto avviene quando membri del personale vengono costretti a fornire del denaro tramite minacce reali o percepite alla salute, alla sicurezza o alla libertà e non rientra nel campo di applicazione del presente documento. La sicurezza e la libertà di una persona sono fondamentali e molti sistemi giuridici non considerano reato l'esecuzione di pagamenti da parte di qualcuno che teme ragionevolmente per la propria salute, sicurezza o libertà o per quella di qualcun altro. L'organizzazione può avere una politica che permette al personale di effettuare pagamenti in circostanze in cui costoro temano un pericolo imminente per la propria salute, sicurezza o libertà o per quella di qualcun altro.

**8.2.2.3** L'organizzazione dovrebbe fornire una guida specifica a qualsiasi membro del personale che subisca tali richieste o domande di tali pagamenti su come evitarli e affrontarli. Tale guida potrebbe, per esempio:

a) specificare le azioni da intraprendere da qualsiasi membro del personale che si trovi ad affrontare tale richiesta di pagamento:

- 1) nel caso di un pagamento agevolativo, chiedendo la prova che tale pagamento sia legittimo e una ricevuta ufficiale per il pagamento e qualora non sia disponibile una prova soddisfacente, rifiutando di effettuare il pagamento;
- 2) nel caso di un pagamento estorto, effettuando il pagamento qualora la sua salute, sicurezza o libertà, o quella di qualcun altro, sia minacciata;

b) specificare le azioni da intraprendere da parte dei membri del personale che abbiano effettuato un pagamento agevolativo o ai quali sia stato estorto un pagamento:

- 1) redigendo un verbale dell'accaduto;
- 2) riferendo l'accaduto ad un manager appropriato o alla funzione di conformità per la prevenzione della corruzione;

c) specificare le azioni da intraprendere da parte dell'organizzazione qualora dei membri del personale abbiano effettuato un pagamento agevolativo o qualora sia stato loro estorto un pagamento:

- 1) nominando un manager competente affinché indaghi sull'accaduto (preferibilmente la funzione di conformità per la prevenzione della corruzione o un manager che sia indipendente rispetto al reparto o alla funzione del membro del personale);

<i>revisione</i>	<i>data</i>	<i>emissione</i>	<i>approvazione</i>	<i>Pagina</i>
0	20/09/2018	RGQ	AU	10 di 28

- 2) registrando debitamente il pagamento nei conti dell'organizzazione;
- 3) se del caso o se previsto dalla legge, segnalando il pagamento alle autorità competenti.

### 8.3 Ragionevolezza e appropriatezza

**8.3.1** La corruzione è spesso celata. Può essere difficile da prevenire, rilevare e affrontare. Riconoscendo tali difficoltà, l'intento complessivo del presente documento è che l'organo direttivo (se presente) e l'alta direzione dell'organizzazione debbano: impegnarsi fattivamente per prevenire, rilevare e affrontare la corruzione in relazione agli affari o alle attività dell'organizzazione; attuare misure, impegnandosi fattivamente, all'interno dell'organizzazione che siano volte a prevenire, rilevare e affrontare la corruzione.

Le misure non possono essere così esose, onerose e burocratiche da renderle insostenibili o da bloccare l'attività commerciale, né possono essere così semplici e inefficaci da consentire facilmente atti di corruzione. Le misure devono essere appropriate al rischio di corruzione e dovrebbero avere una ragionevole probabilità di successo relativamente al loro obiettivo di prevenire, rilevare e affrontare la corruzione.

**8.3.2** Mentre le tipologie di misure per la prevenzione della corruzione che devono essere attuate sono ragionevolmente ben riconoscibili dalle buone pratiche internazionali, e alcune delle quali si rispecchiano nei requisiti della norma, i dettagli delle misure da attuare differiscono abbondantemente a seconda delle circostanze pertinenti. È impossibile prescrivere nel dettaglio ciò che un'organizzazione dovrebbe fare in una particolare circostanza. La qualifica di "ragionevole e appropriata" è stata introdotta in modo da consentire di giudicare ogni circostanza nel merito specifico.

**8.3.3** I seguenti esempi forniscono una guida su come la qualifica di "ragionevole e appropriata" possa applicarsi in relazione a circostanze diverse.

a) Un'organizzazione multinazionale molto grande potrebbe necessitare di affrontare diversi strati di gestione e migliaia di membri del personale. Il proprio sistema di gestione per la prevenzione della corruzione in genere dovrà essere ben più dettagliato di quello di una piccola organizzazione con poco personale.

b) Un'organizzazione che effettui attività in un luogo ad alto rischio di corruzione normalmente necessiterà di una valutazione del rischio di corruzione e di procedure di due diligence molto più organiche e di un livello più elevato di controllo per la prevenzione della corruzione sulle transazioni commerciali in quel luogo rispetto ad un'organizzazione che effettua attività soltanto in un luogo a basso rischio di corruzione, dove la corruzione è relativamente rara.

c) Sebbene il rischio di corruzione esista in relazione a molte transazioni o attività, la valutazione del rischio di corruzione, le procedure di due diligence e i controlli per la prevenzione della corruzione attuati da un'organizzazione coinvolta in una transazione di grande entità o di elevato valore, oppure in attività che implicano un'ampia gamma di soci in affari, è più probabile che siano più organiche di quelle attuate da un'organizzazione in relazione a un'attività commerciale che comprenda la vendita di articoli di modesto valore a molteplici acquirenti o molteplici transazioni di entità minore con una singola parte.

d) Un'organizzazione con uno spettro molto ampio di soci in affari può giungere alla conclusione, nell'ambito della propria valutazione del rischio di corruzione, che sia poco probabile che certe categorie di soci in affari, per esempio gli acquirenti al dettaglio, pongano un rischio di corruzione che non sia superiore allivello basso, e che prendano ciò in considerazione nella progettazione e attuazione del proprio sistema di gestione per la prevenzione della corruzione. Per esempio, è poco probabile che la due diligence sia necessaria, o che sia un controllo proporzionato e ragionevole, in relazione agli acquirenti al dettaglio che acquistano articoli come beni di consumo dall'organizzazione.

**8.3.4** Sebbene il rischio di corruzione esista in relazione a molte transazioni, un'organizzazione dovrebbe attuare un livello di controllo per la prevenzione della corruzione più organico su una transazione ad alto rischio di corruzione rispetto a una transazione con un rischio di corruzione basso. In tale contesto, è importante comprendere che identificare e accettare un basso rischio di corruzione non significa che l'organizzazione accetti il verificarsi di atti di corruzione, ciò vale a dire che il rischio che si verifichi la corruzione (il fatto che possa avvenire un atto di corruzione) non è la stessa cosa che si verifichi effettivamente un atto di corruzione (il fatto di un atto di corruzione in sé). Un'organizzazione può avere tolleranza "zero" per il verificarsi di atti di corruzione pur intraprendendo attività commerciali in situazioni in cui ci possa essere un rischio di corruzione basso, oppure un rischio di corruzione superiore allivello basso (purché siano applicate misure adeguate di limitazione). Una guida ulteriore su tale processo è fornita a seguire.

<i>revisione</i>	<i>data</i>	<i>emissione</i>	<i>approvazione</i>	<i>Pagina</i>
0	20/09/2018	RGQ	AU	11 di 28

#### 8.4 Valutazione del rischio di corruzione

L'intento della valutazione del rischio di corruzione di cui al punto 4.5 della norma è permettere all'organizzazione di costituire una base solida per il proprio sistema di gestione per la prevenzione della corruzione. Tale valutazione identifica i rischi di corruzione su cui si concentra il sistema di gestione, ossia i rischi di corruzione ritenuti essere dall'organizzazione una priorità per la limitazione del rischio di corruzione, l'attuazione del controllo e la destinazione di membri del personale alla conformità per la prevenzione della corruzione, di risorse e di attività. Il modo in cui l'organizzazione effettua la valutazione del rischio di corruzione, la metodologia da applicare, il modo di ponderare e dare priorità ai rischi di corruzione e il livello accettato o tollerato di rischio di corruzione (ossia la propensione al rischio) sono tutti a discrezione dell'organizzazione. In particolare, spetta all'organizzazione stabilire i propri criteri per valutare il rischio di corruzione (per esempio se un rischio sia "basso", "medio" o "alto"); tuttavia, nel fare ciò, l'organizzazione dovrebbe prendere in considerazione la propria politica e i propri obiettivi di prevenzione della corruzione. A seguire è riportato un esempio del modo in cui un'organizzazione può scegliere di effettuare tale valutazione.

a) Selezionare i criteri di valutazione del rischio di corruzione. Per esempio, l'organizzazione può scegliere criteri su tre livelli (ossia "basso", "medio" e "alto"), oppure criteri più dettagliati su cinque o sette livelli o un approccio più approfondito. I criteri spesso prendono in considerazione numerosi fattori, tra cui la natura del rischio di corruzione, la probabilità del verificarsi di atti di corruzione e l'entità delle conseguenze che potrebbero esserci.

b) Valutare i rischi di corruzione posti dalla dimensione e dalla struttura dell'organizzazione.

Una piccola organizzazione con sede in un unico luogo con controlli gestionali centralizzati nelle mani di poche persone può darsi che sia in grado di controllare il proprio rischio di corruzione più facilmente di un'organizzazione molto grande con una struttura decentrata operante in molti luoghi.

c) Esaminare i luoghi e i settori in cui opera l'organizzazione o prevede di operare e valutare il livello di rischio di corruzione che tali luoghi e settori possono porre. Si può utilizzare un vero e proprio indice di corruzione per agevolare tale valutazione. I luoghi o i settori con un rischio di corruzione più elevato possono essere ritenuti dall'organizzazione di rischio, per esempio, "medio" o "alto", il che può comportare che l'organizzazione imponga un livello di controlli più elevato applicabile alle attività dell'organizzazione in tali luoghi o settori.

d) Esaminare la natura, l'entità e la complessità dei tipi di attività e delle operazioni dell'organizzazione.

1) Per esempio, può risultare più semplice controllare il rischio di corruzione dove un'organizzazione effettua una modesta attività manifatturiera in un unico luogo rispetto a un'organizzazione che è coinvolta in numerosi e ampi progetti edili in più luoghi.

2) Alcune attività possono comportare rischi di corruzione specifici, per esempio accordi compensativi in base a cui il governo che acquista i prodotti o i servizi richieda che il fornitore reinvesta una parte del valore dell'appalto nel paese che ha fatto l'acquisto. L'organizzazione dovrebbe intraprendere le misure appropriate per prevenire che gli accordi compensativi costituiscano atti di corruzione.

e) Esaminare i tipi di soci in affari dell'organizzazione esistenti e attuali per categoria e valutare in linea di principio il rischio di corruzione che pongono. Per esempio:

1) L'organizzazione può avere un numero elevato di acquirenti che acquistano prodotti di valore molto modesto dall'organizzazione e che in pratica pongono un rischio di corruzione minimo all'organizzazione. In tal caso, l'organizzazione ha facoltà di ritenere tali acquirenti a basso rischio di corruzione e può determinare che tali acquirenti non necessitino di controlli per la prevenzione della corruzione specifici indirizzati a loro. In alternativa, l'organizzazione può rapportarsi con gli acquirenti che acquistano prodotti di elevato valore dall'organizzazione e che possono porre un rischio di corruzione significativo (per esempio il rischio che richiedano all'organizzazione tangenti in cambio di pagamenti e permessi). Questi tipi di acquirenti possono essere considerati di rischio "medio" o "alto" e possono richiedere un livello di controlli per la prevenzione della corruzione più elevato da parte dell'organizzazione.

2) Diverse categorie di fornitori possono porre livelli diversi di rischio di corruzione.

Per esempio, i fornitori con una portata di lavoro molto ampia o che potrebbero essere in contatto con i clienti dell'organizzazione, con gli acquirenti o con i pubblici ufficiali pertinenti possono porre un rischio di corruzione "medio" o "alto". Alcune categorie di fornitori può darsi che siano di rischio "basso", per esempio i fornitori con sede in luoghi a basso rischio di corruzione che non si interfacciano con pubblici ufficiali rilevanti per la transazione o i clienti o gli acquirenti dell'organizzazione. Alcune categorie di fornitori possono porre un rischio di corruzione "molto basso", per esempio i fornitori di piccole quantità di articoli di modesto valore, i servizi di acquisto online per voli aerei o alberghi.

<i>revisione</i>	<i>data</i>	<i>emissione</i>	<i>approvazione</i>	<i>Pagina</i>
0	20/09/2018	RGQ	AU	12 di 28

L'organizzazione può darsi che giunga alla conclusione che i controlli per la prevenzione della corruzione specifici non necessitano di essere applicati nei confronti di tali fornitori a basso o molto basso rischio di corruzione.

3) È più probabile che gli agenti o gli intermediari che interagiscono con i clienti dell'organizzazione o con i pubblici ufficiali per conto dell'organizzazione pongano un rischio di corruzione "medio" o "alto", in particolare se sono pagati su commissione o con una tariffa in base all'esito positivo.

f) Esaminare la natura e la frequenza delle interazioni con pubblici ufficiali connazionali o stranieri che pongono un rischio di corruzione, per esempio le interazioni con pubblici ufficiali responsabili di emettere permessi e approvazioni, possono rappresentare un rischio di corruzione.

g) Esaminare gli obblighi vigenti in base a leggi, regolamenti, contratti e gli adempimenti e i doveri professionali, per esempio il divieto o la limitazione di intrattenere i pubblici ufficiali o l'utilizzo di agenti.

h) Considerare la misura in cui l'organizzazione è in grado di influenzare o controllare i rischi valutati.

I rischi di corruzione di cui sopra sono interrelati. Per esempio, i fornitori della medesima categoria possono rappresentare rischi di corruzione differenti a seconda del luogo in cui operano.

**8.4.2** Dopo avere valutato i rischi di corruzione pertinenti, l'organizzazione può determinare il tipo e il livello di controlli per la prevenzione della corruzione applicati a ogni categoria di rischio e può valutare se i controlli in essere siano adeguati. In caso contrario, i controlli possono essere debitamente migliorati. Per esempio, è probabile che un livello di controlli più elevato sia attuato in base a luoghi a più alto rischio di corruzione e a categorie di soci in affari a rischio di corruzione più alto. L'organizzazione può determinare che sia accettabile avere un basso livello di controllo su attività o soci in affari a basso rischio di corruzione. Alcuni dei requisiti del presente documento escludono espressamente la necessità di applicare quei requisiti ad attività o soci in affari a basso rischio di corruzione (sebbene l'organizzazione abbia facoltà di scegliere di applicarli se lo desidera).

**8.4.3** L'organizzazione può modificare la natura della transazione, del progetto, dell'attività o della relazione in modo che la natura e l'entità del rischio di corruzione sia abbassato a un livello che possa essere gestito adeguatamente dai controlli per la prevenzione della corruzione in essere, potenziati o aggiuntivi.

**8.4.4** Tale esercizio di valutazione del rischio di corruzione non è inteso come un esercizio estensivo ed eccessivamente complesso e i risultati della valutazione non devono necessariamente dimostrarsi corretti (per esempio una transazione valutata come rischio di corruzione basso può rivelare la presenza di atti di corruzione). Per quanto ragionevolmente fattibile, i risultati della valutazione del rischio di corruzione dovrebbero rispecchiare i rischi di corruzione attuali cui l'organizzazione è sottoposta. L'esercizio dovrebbe essere progettato come strumento per aiutare l'organizzazione a valutare il proprio rischio di corruzione e a stabilirne le priorità e dovrebbe essere sottoposto a riesame e verifica periodicamente sulla base delle modifiche avvenute nell'organizzazione o delle circostanze (per esempio in caso di nuovi mercati o prodotti, requisiti di legge ed esperienza maturata).

Nota. Ulteriori istruzioni sono fornite nella ISO 31000.

## 8.5 Ruoli e responsabilità dell'organo direttivo e dell'alta dirigenza

**8.5.1** Molte organizzazioni hanno alcune forme di organo direttivo (per esempio un consiglio di amministrazione o un consiglio di vigilanza) che ha responsabilità generali di supervisione relativamente all'organizzazione. Tali responsabilità comprendono la supervisione del sistema di gestione per la prevenzione della corruzione dell'organizzazione. Tuttavia, l'organo direttivo generalmente non esercita una direzione quotidiana sulle attività dell'organizzazione. Questo è il ruolo della direzione esecutiva (per esempio dell'amministratore delegato o del direttore operativo) che nel presente documento è indicato dall'espressione "alta direzione". Per quanto concerne il sistema di gestione per la prevenzione della corruzione, l'organo direttivo dovrebbe essere a conoscenza del contenuto e del funzionamento del sistema di gestione e dovrebbe esercitare una

supervisione ragionevole in relazione all'adeguatezza, all'efficacia e all'attuazione del sistema di gestione. Dovrebbe ricevere regolarmente informazioni a proposito della prestazione del sistema di gestione tramite il processo di riesame organizzativo (ciò potrebbe riferirsi all'intero organo direttivo o a una commissione dell'organo, come la commissione audit). In tal senso, la funzione di conformità per la prevenzione della corruzione dovrebbe essere in grado di comunicare le informazioni sul sistema di gestione direttamente all'organo direttivo (o alla commissione competente).

**8.5.2** Può darsi che alcune organizzazioni, specialmente quelle piccole, non dispongano di un organo direttivo separato, o che i ruoli dell'organo direttivo e della gestione esecutiva siano concentrati in un solo

<i>revisione</i>	<i>data</i>	<i>emissione</i>	<i>approvazione</i>	<i>Pagina</i>
0	20/09/2018	RGQ	AU	13 di 28

gruppo o in un unico individuo. In tali casi, il gruppo o l'individuo detiene le responsabilità assegnate nel presente documento all'alta direzione e all'organo direttivo.

Nota. L'impegno alla leadership a volte è identificato dalle espressioni "lone at the top" o "lone from the top"

## 8.6 Funzione di conformità per la prevenzione della corruzione

**8.6.1** Il numero delle persone che lavorano nella funzione di conformità per la prevenzione della corruzione dipende da fattori quali le dimensioni dell'organizzazione, l'entità del rischio di corruzione cui è sottoposta l'organizzazione e il restante carico di lavoro della funzione. Nelle organizzazioni piccole, è probabile che la funzione di conformità per la prevenzione della corruzione sia una sola persona a cui è affidata la responsabilità a tempo parziale e che coniuga tale responsabilità con altre responsabilità. Laddove l'entità del rischio di corruzione e il carico di lavoro risultante lo giustificano, la funzione di conformità per la prevenzione della corruzione può essere una persona a cui è assegnata tale responsabilità a tempo pieno. Nelle organizzazioni grandi, è probabile che la funzione sia ricoperta da diverse persone. Alcune organizzazioni possono assegnare la responsabilità a una commissione che incarni una serie di professionalità in materia. Alcune organizzazioni possono scegliere di utilizzare una parte terza per svolgere in tutto o in parte la funzione di conformità per la prevenzione della corruzione e ciò è accettabile, ammesso che un manager competente dell'organizzazione mantenga la responsabilità generale e l'autorità in merito alla funzione di conformità per la prevenzione della corruzione e che supervisioni i servizi forniti dalla parte terza.

**8.6.2** La norma ISO 37001 richiede che la funzione di conformità per la prevenzione della corruzione sia ricoperta da una o più persone che possiedano competenze, status, autorità e indipendenza appropriati. A tal proposito:

- per "competenza" si intende che le persone pertinenti abbiano l'istruzione, la formazione o l'esperienza adeguate, l'abilità personale di affrontare i requisiti del ruolo e la capacità di imparare quanto concerne il ruolo e che lo svolgano adeguatamente;
- per "status" si intende che verosimilmente gli altri membri del personale ascoltino e rispettino le opinioni della persona a cui è assegnata la responsabilità di conformità;
- per "autorità" si intende che alle persone pertinenti a cui è affidata la responsabilità di conformità siano concessi sufficienti poteri dall'organo direttivo (se presente) e dall'alta direzione in modo da essere in grado di espletare efficacemente le responsabilità di conformità;
- per "indipendenza" si intende che le persone in questione a cui è assegnata la responsabilità di conformità non siano, per quanto possibile, personalmente coinvolte nelle attività dell'organizzazione che sono esposte al rischio di corruzione. Ciò può essere raggiunto più facilmente se l'organizzazione ha nominato una persona per assumere tale ruolo a tempo pieno, ma è più difficoltoso per una piccola organizzazione che ha nominato una persona perché coniughi il ruolo di conformità con altre funzioni. Laddove la funzione di conformità per la prevenzione della corruzione sia a tempo parziale, il ruolo non dovrebbe essere assunto da un individuo che sia esposto alla corruzione nello svolgimento della sua funzione primaria. Nel caso di un'organizzazione molto piccola dove può risultare più complicato raggiungere l'indipendenza, la persona appropriata dovrebbe fare tutto quanto nelle sue possibilità per separare le altre responsabilità dalle sue responsabilità di conformità in modo da essere imparziale.

È importante che la funzione di conformità per la prevenzione della corruzione abbia accesso diretto all'alta direzione e all'organo direttivo (se presente), al fine di comunicare le informazioni pertinenti. La funzione non dovrebbe solo riferire a un altro manager nella catena il quale poi a propria volta riferisce all'alta direzione, in quanto ciò aumenta il rischio che il messaggio fornito dalla funzione di conformità per la prevenzione della corruzione non sia recepito in modo completo e chiaro dall'alta direzione. La funzione di conformità per la prevenzione della corruzione dovrebbe anche poter intrattenere scambi comunicativi diretti con l'organo direttivo (se presente), senza dover passare per l'alta direzione. Ciò potrebbe riferirsi o all'intero organo direttivo al completo (per esempio al consiglio di amministrazione o al consiglio di sorveglianza) oppure a una commissione speciale competente dell'organo direttivo o dell'alta direzione (per esempio una commissione audit o etica).

**8.6.4** La responsabilità primaria della funzione di conformità per la prevenzione della corruzione è la supervisione della progettazione e dell'attuazione del sistema di gestione per la prevenzione della corruzione. Ciò non dovrebbe essere confuso con la responsabilità diretta della prestazione per la prevenzione della corruzione dell'organizzazione e con la conformità alle leggi per la prevenzione della corruzione vigenti. Ognuno è responsabile per la propria condotta in modo che sia etica e conforme, ivi compresa l'osservanza dei requisiti del sistema di gestione per la prevenzione della corruzione dell'organizzazione e delle leggi per la

<i>revisione</i>	<i>data</i>	<i>emissione</i>	<i>approvazione</i>	<i>Pagina</i>
0	20/09/2018	RGQ	AU	14 di 28

prevenzione della corruzione. È particolarmente importante che la direzione assuma un ruolo di leadership nel raggiungimento della conformità nelle parti dell'organizzazione per cui è responsabile.  
Nota. Ulteriori istruzioni sono fornite nella ISO 19600.

## 8.7 Risorse

Le risorse necessarie dipendono da fattori come le dimensioni dell'organizzazione, la natura delle sue operazioni e i rischi di corruzione cui è sottoposta. Di seguito sono riportati alcuni esempi di risorse.

- Risorse umane: Dovrebbe esserci membri del personale a sufficienza che siano in grado di dedicare sufficiente tempo alle loro responsabilità per la prevenzione della corruzione in modo che il sistema di gestione per la prevenzione della corruzione possa funzionare efficacemente. Ciò comprende l'assegnazione di persone a sufficienza (interne o esterne) alla funzione di conformità per la prevenzione della corruzione.
- Risorse fisiche: Dovrebbero esserci risorse fisiche a sufficienza nell'organizzazione, comprese quelle nella funzione di conformità per la prevenzione della corruzione, per consentire al sistema di gestione per la prevenzione della corruzione di funzionare efficacemente, per esempio spazio adibito a ufficio, mobili, hardware e software informatico, materiali formativi, telefoni e cancelleria.
- Risorse finanziarie: Dovrebbe esserci un budget sufficiente, compreso quello per la funzione di conformità per la prevenzione della corruzione, per consentire al sistema di gestione di prevenzione della corruzione di funzionare efficacemente.

## 8.8 Procedure di assunzione

### 8.8.1 Due diligence sul personale

Nello svolgimento della due diligence sulle persone precedentemente alla loro nomina a personale, l'organizzazione, in base alle funzioni proposte alle funzioni e al rischio di corruzione corrispondente, può adottare misure come:

- discutere la politica per la prevenzione della corruzione dell'organizzazione con i potenziali nuovi membri del personale durante il colloquio, facendosi un'idea se sembrano comprendere e accettare l'importanza della conformità;
- intraprendere azioni ragionevoli per verificare che le qualifiche dei potenziali nuovi membri del personale siano accurate;
- intraprendere azioni ragionevoli per ottenere referenze soddisfacenti dai datori di lavoro precedenti dei potenziali nuovi membri del personale;
- intraprendere azioni ragionevoli per determinare se i potenziali nuovi membri del personale siano stati coinvolti in atti di corruzione;
- intraprendere azioni ragionevoli per verificare che l'organizzazione non stia offrendo lavoro a potenziali nuovi membri del personale per aver, durante l'impiego precedente, favorito illecitamente l'organizzazione;
- verificare che l'obiettivo dell'offerta di lavoro ai potenziali nuovi membri del personale non sia quello di assicurare un trattamento favorevole improprio all'organizzazione;
- intraprendere azioni ragionevoli per identificare le relazioni dei potenziali nuovi membri del personale con i pubblici ufficiali.

### 8.8.2 Bonus per la prestazione

Gli accordi sulla retribuzione, compresi bonus e incentivi, possono spingere, anche inavvertitamente, il personale a partecipare ad atti di corruzione. Per esempio, se un manager riceve un bonus basato sull'aggiudicazione di un appalto all'organizzazione, il manager potrebbe essere tentato a pagare una tangente o a chiudere un occhio su un agente o un socio in joint venture che paghi una tangente al fine da assicurarsi l'aggiudicazione dell'appalto. Il medesimo risultato potrebbe verificarsi se si mette troppa pressione sulla prestazione di un manager (per esempio se il manager potrebbe essere licenziato per non essere riuscito a raggiungere obiettivi di vendita oltremodo ambiziosi). L'organizzazione deve prestare un'attenzione accurata a questi aspetti della retribuzione per garantire, per quanto ragionevole, che non fungano da incentivi alla corruzione.

Le valutazioni, le promozioni, i bonus e le altre ricompense del personale potrebbero essere utilizzate come incentivi affinché il personale si comporti conformemente alla politica e al sistema di gestione per la prevenzione della corruzione dell'organizzazione. Ciononostante, l'organizzazione deve essere cauta in tal caso, poiché la minaccia di perdere il bonus, ecc., può portare il personale a nascondere le criticità nel sistema di gestione per la prevenzione della corruzione.

Il personale dovrebbe essere reso consapevole del fatto che gli inadempimenti al sistema di gestione per la prevenzione della corruzione volti a migliorare la valutazione della propria prestazione in altri campi (per

<i>revisione</i>	<i>data</i>	<i>emissione</i>	<i>approvazione</i>	<i>Pagina</i>
0	20/09/2018	RGQ	AU	15 di 28

esempio il raggiungimento degli obiettivi di vendita) non sono accettabili e potrebbero risultare in azioni correttive e/o disciplinari.

### 8.8.3 Conflitti di interessi

L'organizzazione dovrebbe identificare e valutare il rischio di conflitti di interessi interni ed esterni. L'organizzazione dovrebbe informare in modo chiaro tutto il personale del loro dovere di riferire qualsiasi conflitto di interessi effettivo o potenziale come i legami famigliari, economici o altro che siano direttamente o indirettamente legati alla loro linea di lavoro. Ciò aiuta l'organizzazione a identificare le situazioni in cui il personale potrebbe favorire oppure omettere di prevenire o di riferire atti di corruzione, per esempio:

- a) quando il responsabile delle vendite dell'organizzazione è legato al responsabile degli approvvigionamenti dell'acquirente, oppure
- b) quando un manager di linea dell'organizzazione ha un interesse economico personale nelle attività commerciali del concorrente.

L'organizzazione dovrebbe preferibilmente tenere traccia di ogni circostanza di conflitti di interesse effettivi o potenziali e se siano state intraprese azioni per limitare tale conflitto.

### 8.8.4 Corruzione del personale dell'organizzazione

**8.8.4.1** Le misure necessarie per prevenire, rilevare e affrontare il rischio che il personale dell'organizzazione corrompa altri per conto dell'organizzazione ("corruzione in uscita") può essere diverso dalle misure utilizzate per prevenire, rilevare e affrontare il rischio di corruzione del personale dell'organizzazione ("corruzione in entrata"). Per esempio, la capacità di identificare e limitare il rischio di corruzione in entrata può essere significativamente ridotta dalla disponibilità delle informazioni che non sono sotto il controllo dell'organizzazione (per esempio i conti correnti bancari dei dipendenti e i dati delle transazioni delle carte di credito), delle leggi vigenti (per esempio le normative sulla privacy) o di altri fattori. Di conseguenza il numero e il tipo di controlli disponibili all'organizzazione per contenere il rischio di corruzione in uscita può essere preponderante al numero di controlli che può effettuare per limitare il rischio di corruzione in entrata.

**8.8.4.2** È più probabile che accadano atti di corruzione del personale dell'organizzazione nei confronti di quei membri del personale che sono in grado di assumere o influenzare decisioni per conto dell'organizzazione (per esempio un responsabile degli approvvigionamenti che può aggiudicare gli appalti; un supervisore che può approvare il lavoro svolto; un manager che può nominare il personale o approvare salari o bonus; un impiegato che prepara i documenti per la concessione di licenze o permessi). Visto che è probabile che la tangente sia accettata dai membri del personale al di fuori del campo di applicazione dei sistemi o dei controlli dell'organizzazione, la capacità dell'organizzazione di prevenire o rilevare tali tangenti può essere limitata.

**8.8.4.3** In aggiunta alle misure di cui ai punti 8.8.1 e 8.8.3, il rischio di corruzione in entrata potrebbe essere limitato dai requisiti seguenti del presente documento concernente tale rischio:

- a) la politica per la prevenzione della corruzione dell'organizzazione (vedere punto 5.2 della norma) dovrebbe vietare esplicitamente la richiesta e l'accettazione di tangenti da parte del personale dell'organizzazione e di chiunque operi per conto dell'organizzazione;
- b) materiali guida e formativi (vedere punto 7.3 della norma) dovrebbero rinforzare il divieto di richiedere e accettare tangenti, includendo:
  - 1) istruzioni per la segnalazione di sospetti di corruzione (vedere punto 8.9 della norma);
  - 2) l'enfasi posta sulla politica di non ritorsione dell'organizzazione (vedere punto 8.9);
- c) la politica dell'organizzazione sui regali e l'ospitalità (vedere punto 8.7 della norma) dovrebbe limitare l'accettazione da parte del personale di regali e ospitalità;
- d) la pubblicazione sul sito web dell'organizzazione della politica di prevenzione della corruzione dell'organizzazione e i dettagli di come segnalare atti di corruzione aiutano a stabilire le aspettative dei soci in affari, in modo da diminuire la probabilità che i soci in affari propongano tangenti o che membri del personale dell'organizzazione le richiedano o le accettino;
- e) controlli (vedere punto 8.3 e 8.4 della norma) che prevedano, per esempio, l'utilizzo di fornitori approvati, gare d'appalto, almeno due firme sulle aggiudicazioni di appalto, approvazioni dei lavori, ecc., ridimensionano il rischio di aggiudicazioni, approvazioni, pagamenti o benefici oggetto di corruzione.

**8.8.4.4** L'organizzazione ha facoltà di adottare procedure di audit per identificare le modalità in cui il personale possa sfruttare i punti deboli dei controlli in essere a proprio vantaggio personale. Procedure a titolo di esempio possono essere:

<i>revisione</i>	<i>data</i>	<i>emissione</i>	<i>approvazione</i>	<i>Pagina</i>
0	20/09/2018	RGQ	AU	16 di 28

- a) riesaminare i documenti relativi alle retribuzioni onde scoprire registrazioni fantasma o duplici del personale;
- b) riesaminare i giustificativi delle spese di lavoro del personale per identificare spese atipiche;
- c) incrociare le informazioni dei documenti relativi alle retribuzioni del personale (per esempio i numeri e gli indirizzi dei conti correnti bancari personali) con le informazioni sui conti correnti e gli indirizzi nel file master venditori dell'organizzazione per identificare scenari potenziali di conflitto di interessi.

#### **8.8.5 Staff o lavoratori temporanei**

In alcuni casi, lo staff o i lavoratori temporanei possono essere forniti all'organizzazione da fornitori di manodopera o da altri soci in affari. In tal caso, l'organizzazione dovrebbe determinare se il rischio di corruzione posto da tali membri dello staff o lavoratori temporanei (se presenti) sia affrontato adeguatamente considerando lo staff o i lavoratori temporanei come proprio personale ai fini di formazione e controllo, o se sia il caso di applicare controlli appropriati tramite il socio in affari che fornisce lo staff o i lavoratori temporanei.

### **A.9 Consapevolezza e formazione**

**A.9.1** Intento della formazione è assicurare che i membri del personale pertinenti comprendano, in base a quanto appropriato per il loro ruolo all'interno o verso l'organizzazione, quanto segue:

- a) i rischi di corruzione cui loro e l'organizzazione sono sottoposti;
- b) la politica di prevenzione della corruzione;
- c) gli aspetti del sistema di gestione per la prevenzione della corruzione pertinenti al loro ruolo;
- d) qualsivoglia azione preventiva e di segnalazione necessaria che essi devono intraprendere in relazione a qualsiasi rischio di corruzione o sospetta corruzione.

**8.9.2** La formalità e l'entità della formazione dipende dalle dimensioni dell'organizzazione e dai rischi di corruzione affrontati. Essa può essere svolta come modulo online o con metodi frontali (per esempio sessioni in classe, seminari, discussioni in tavole rotonde tra i membri interessati del personale o tramite sessioni individuali). Il metodo di formazione è meno importante del risultato, che dovrebbe consistere nel fare comprendere a tutti i membri del personale interessati le tematiche di cui al punto 8.9.1 del presente documento.

**8.9.3** È consigliabile la formazione frontale per l'organo direttivo (se presente) e qualsiasi membro del personale (indipendentemente dalla posizione o dal grado gerarchico nell'organizzazione) e per i soci in affari che sono coinvolti in operazioni e processi con un rischio di corruzione superiore all'livello basso.

**8.9.4** Se le persone pertinenti a cui è assegnata la funzione di conformità per la prevenzione della corruzione non hanno una sufficiente esperienza in materia, l'organizzazione dovrebbe fornire qualsiasi tipo di formazione necessaria a tali persone per espletare in modo adeguato la funzione di conformità per la prevenzione della corruzione.

**8.9.5** La formazione può avere luogo come formazione sulla prevenzione della corruzione a se stante o può far parte della formazione o del programma introduttivo complessivo dell'organizzazione sulla conformità e l'etica.

**8.9.6** Il contenuto della formazione può essere adattato al ruolo del personale. I membri del personale che non sono sottoposti a rischi significativi di corruzione nell'ambito del loro ruolo potrebbero ricevere una formazione molto semplice sulla politica dell'organizzazione, in modo che comprendano tale politica e sappiano cosa fare se notano una potenziale violazione. I membri del personale il cui ruolo implichi un rischio alto di corruzione dovrebbero ricevere una formazione più dettagliata.

**8.9.7** La formazione dovrebbe essere ripetuta ogniqualvolta sia necessario in modo che il personale sia al passo con le politiche e le procedure dell'organizzazione, con qualsiasi sviluppo in relazione al rispettivo ruolo e con qualsiasi modifica legislativa.

**8.9.8** L'applicazione dei requisiti di formazione e consapevolezza ai soci in affari identificati in base ai requisiti di cui al punto 7.3 della norma pone sfide particolari poiché i dipendenti di tali soci in affari in genere non lavorano direttamente per l'organizzazione e l'organizzazione normalmente non ha accesso diretto a tali dipendenti a fini formativi. La formazione effettiva dei dipendenti impiegati dai soci in affari normalmente è svolta dai soci in affari stessi o da altre parti incaricate a tal fine. È importante che i dipendenti che lavorano per i soci in affari che pongono un rischio di corruzione superiore al livello basso all'organizzazione siano consapevoli della questione e ricevano una formazione ragionevolmente volta a ridurre tale rischio. Il contenuto della norma richiede che l'organizzazione, come minimo, identifichi i soci in affari i cui dipendenti dovrebbero ricevere la formazione per la prevenzione della corruzione, stabilisca quale dovrebbe essere il contenuto minimo di tale formazione e che tale formazione dovrebbe essere svolta. La

<i>revisione</i>	<i>data</i>	<i>emissione</i>	<i>approvazione</i>	<i>Pagina</i>
0	20/09/2018	RGQ	AU	17 di 28

formazione in sé può essere fornita dai soci in affari, da altre parti designate oppure, se l'organizzazione lo decide, da parte dell'organizzazione stessa. L'organizzazione può comunicare tali obblighi ai propri soci in affari in varie modalità, tra cui inserendola in accordi contrattuali.

## 8.10 Due diligence

**8.10.1** Lo scopo di condurre la due diligence su determinate transazioni, progetti, attività, soci in affari o membri del personale di un'organizzazione è quello di valutare ulteriormente la portata, l'entità e la natura di rischi di corruzione più che bassi identificati nell'ambito della valutazione del rischio dell'organizzazione (vedere punto 4.5 della norma). Ciò è inoltre finalizzato a fungere da controllo aggiuntivo e mirato nella prevenzione e nel rilevamento del rischio di corruzione e informa la decisione dell'organizzazione sull'eventualità di procrastinare, interrompere o revisionare tali transazioni, progetti o relazioni con i soci in affari o membri del personale.

**8.10.2** In relazione a progetti, transazioni e attività, tra i fattori che l'organizzazione può trovare utili da valutare vi sono:

- a) la struttura, la natura e la complessità (per esempio la vendita diretta o indiretta, il livello di sconto, le procedure di aggiudicazione degli appalti e dei bandi di gara);
- b) gli accordi su finanziamenti e pagamenti;
- c) il campo di coinvolgimento dell'organizzazione e le risorse disponibili;
- d) il livello di controllo e di visibilità;
- e) i soci in affari e le altre parti terze coinvolte (compresi i pubblici ufficiali);
- f) i legami tra qualsiasi parte di cui al precedente punto e) ed i pubblici ufficiali;
- g) la competenza e le qualifiche delle parti coinvolte;
- h) la reputazione del cliente;
- i) l'ubicazione;
- j) le recensioni del mercato o della stampa.

**8.10.3** In relazione alla possibile due diligence sui soci in affari:

- a) i fattori che l'organizzazione può trovare utili da valutare in relazione a un socio in affari comprendono:
  - 1) se il socio in affari sia un'entità commerciale legittima, come dimostrato da indicatori quali i documenti di iscrizione al registro delle imprese, la registrazione delle scritture contabili annuali, il numero di partita IVA, la quotazione in borsa;
  - 2) se il socio in affari abbia le qualifiche, l'esperienza e le risorse necessarie per condurre le attività commerciali per cui è stato assegnato l'appalto;
  - 3) se e in che misura il socio in affari abbia un sistema di gestione per la prevenzione della corruzione;
  - 4) se il socio in affari abbia la fama di coinvolgimento in atti di corruzione, condotte fraudolente, illeciti o condotte scorrette simili, oppure se sia stato indagato, condannato, sanzionato o escluso da procedure per corruzione o reati analoghi;
  - 5) l'identità degli azionisti (compresi gli aventi diritto economico) e l'alta direzione dei soci in affari e se essi:
    - i) abbiano la fama di coinvolgimento in atti di corruzione, condotte fraudolente, illeciti o condotte scorrette simili;
    - ii) siano stati indagati, condannati, sanzionati o esclusi da procedure per corruzione o reati analoghi;
    - iii) abbiano qualsiasi legame diretto o indiretto col cliente o con l'acquirente dell'organizzazione oppure con un pubblico ufficiale pertinente che potrebbe portare ad atti di corruzione (ciò comprenderebbe le persone che non sono pubblici ufficiali di per sé, ma che possono essere legate direttamente o indirettamente a pubblici ufficiali, a candidati a cariche pubbliche, ecc.);
  - 6) la struttura degli accordi sulle transazioni e sui pagamenti;
- b) la natura, il tipo e l'entità della due diligence effettuata dipende da fattori come la capacità dell'organizzazione di ottenere informazioni sufficienti, i costi per l'ottenimento delle informazioni e l'entità del possibile rischio di corruzione posto dalla relazione;
- c) le procedure di due diligence attuate dall'organizzazione in merito ai propri soci in affari dovrebbero essere coerenti tra livelli di rischi di corruzione simili (è probabile che i soci in affari ad alto rischio di corruzione in luoghi o mercati in cui c'è un alto rischio di corruzione richiedano un livello di due diligence significativamente più elevato rispetto a soci a basso rischio di corruzione in luoghi o mercati con un basso rischio di corruzione);
- d) è probabile che tipi diversi di soci in affari richiedano livelli diversi di due diligence, per esempio:

<i>revisione</i>	<i>data</i>	<i>emissione</i>	<i>approvazione</i>	<i>Pagina</i>
0	20/09/2018	RGQ	AU	18 di 28

1) dal punto di vista della responsabilità legale e finanziaria potenziale dell'organizzazione, i soci in affari pongono all'organizzazione un rischio di corruzione maggiore quando essi agiscono per conto dell'organizzazione o per il suo vantaggio rispetto a quando forniscono all'organizzazione prodotti o servizi. Per esempio, un agente che si occupa di assistere un'organizzazione affinché ottenga l'aggiudicazione di un appalto potrebbe pagare una tangente a un manager dell'acquirente dell'organizzazione per agevolare l'organizzazione stessa a vincere l'appalto e, in questo modo, potrebbe portare l'organizzazione a essere responsabile dell'atto di corruzione dell'agente. Di conseguenza, è probabile che la due diligence dell'organizzazione nei confronti dell'agente sia la più completa possibile. Dall'altro lato, un fornitore che vende attrezzatura o materiale all'organizzazione e che non ha a che fare con gli acquirenti dell'organizzazione o con i pubblici ufficiali che riguardano le attività dell'organizzazione è meno probabile che sia in grado di pagare una tangente per conto dell'organizzazione o a suo vantaggio, quindi il livello di due diligence nei confronti di tale fornitore potrebbe essere minore;

2) anche il livello di influenza che l'organizzazione ha sui propri soci in affari condiziona la capacità dell'organizzazione di ottenere informazioni direttamente da quei soci in affari nell'ambito della propria due diligence. Può essere relativamente semplice per un'organizzazione richiedere ai propri agenti o partner di joint venture di fornire informazioni approfondite su di loro nell'ambito di un esercizio di due diligence precedente all'impegno dell'organizzazione di lavorare con loro, così che l'organizzazione abbia un margine di scelta per stabilire con chi stipulare un contratto in tale situazione. Tuttavia, può essere più difficoltoso per un'organizzazione richiedere a un cliente o a un acquirente di fornire informazioni riguardo loro stessi o di completare questionari di due diligence. Ciò potrebbe essere dovuto al fatto che l'organizzazione non avrebbe sufficiente influenza sul cliente o sull'acquirente per essere in grado di fare ciò (per esempio nel caso in cui l'organizzazione sia coinvolta in un bando di gara al fine di fornire servizi all'acquirente);

e) la due diligence effettuata dall'organizzazione sui propri soci in affari può includere, per esempio:

1) un questionario inviato al socio in affari in cui si chiede di rispondere a domande concernenti il punto 8.10.3 a);

2) un ricerca in internet sul socio in affari e sui propri azionisti e alta dirigenza per scoprire informazioni legate a qualsiasi atto di corruzione;

3) la ricerca in fonti governative, giudiziarie e internazionali adeguate di informazioni in materia;

4) controlli in liste pubbliche di esclusione di organizzazioni che hanno limitazioni o divieti a partecipare ad appalti di enti pubblici o governativi stilati da governi nazionali o locali o da istituzioni multilaterali, come la Banca Mondiale;

5) richieste a altre parti pertinenti relativamente alla reputazione etica del socio in affari;

6) la nomina di altre persone od organizzazioni con esperienza in materia a supporto del processo di due diligence;

f) si possono porre al socio in affari domande ulteriori sulla base dei risultati della due diligence preliminari (per esempio chiedere chiarimenti circa informazioni sfavorevoli).

**8.10.4** La due diligence non è uno strumento perfetto. L'assenza di informazioni negative non significa necessariamente che il socio in affari non ponga un rischio di corruzione. Le informazioni negative non significano necessariamente che il socio in affari ponga un rischio di corruzione. Tuttavia, i risultati devono essere valutati attentamente e l'organizzazione deve fornire un giudizio razionale sulla base dei fatti che ha a disposizione. L'intento complessivo è che l'organizzazione faccia richieste ragionevoli e appropriate sul socio in affari, considerando le attività che il socio in affari svolgerebbe e il rischio di corruzione intrinseco a tali attività, in modo da costruire un giudizio ragionevole sul livello di rischio di corruzione a cui è sottoposta l'organizzazione qualora lavori con il socio in affari.

**8.10.5** La due diligence sul personale è trattata al punto 8.8.1.

### 8.11 Controlli finanziari

Per controlli finanziari si intendono i sistemi e i processi di gestione attuati dall'organizzazione per gestire debitamente le proprie transazioni finanziarie e per registrare tali transazioni in modo accurato, completo e puntuale. A seconda delle dimensioni dell'organizzazione e della transazione, i controlli finanziari attuati da un'organizzazione che possono ridurre il rischio di corruzione potrebbero comprendere, per esempio:

a) l'attuazione di una separazione di compiti, in modo che un pagamento non possa essere avviato e approvato dalla stessa persona;

<i>revisione</i>	<i>data</i>	<i>emissione</i>	<i>approvazione</i>	<i>Pagina</i>
0	20/09/2018	RGQ	AU	19 di 28

- b) l'attuazione di livelli gerarchici appropriati di autorità per l'approvazione di un pagamento (in modo che le transazioni più consistenti richiedano l'approvazione di un più alto livello di management);
- c) la verifica che la nomina del beneficiario e il lavoro o i servizi effettuati siano stati approvati dai meccanismi di approvazione pertinenti dell'organizzazione;
- d) la richiesta di almeno due firme sulle approvazioni di pagamento;
- e) la richiesta della documentazione di supporto appropriata in allegato alle approvazioni di pagamento;
- f) la restrizione dell'uso del contante e l'attuazione di metodi efficaci di controllo del contante;
- g) la richiesta che le classificazioni e le descrizioni dei pagamenti nei conti siano accurate e chiare;
- h) l'attuazione del riesame gestionale periodico delle transazioni finanziarie significative;
- i) l'attuazione degli audit finanziari periodici e indipendenti e l'avvicendamento, a cadenze regolari, della persona o dell'organizzazione che esegue l'audit.

### 8.12 Controlli non finanziari

Per controlli non finanziari si intendono i sistemi e i processi di gestione attuati da parte dell'organizzazione per aiutare a garantire che gli aspetti di aggiudicazione, operativi, commerciali e gli altri aspetti non finanziari delle proprie attività siano gestite adeguatamente. A seconda delle dimensioni dell'organizzazione e della transazione, i controlli sull'aggiudicazione, operativi, commerciali e non finanziari attuati da un'organizzazione che possono ridurre il rischio di corruzione potrebbero comprendere, per esempio, i seguenti controlli:

- a) l'utilizzo di appaltatori, sub-appaltatori, fornitori e consulenti approvati che si siano sottoposti a un processo di pre-candidatura durante il quale si valuta la probabilità del loro coinvolgimento in atti di corruzione; è probabile che tale processo includa il tipo di due diligence specificata al punto A.I O;
- b) valutare:
  - 1) la necessità e la legittimità dei servizi forniti da un socio in affari (eccetto clienti e acquirenti) all'organizzazione,
  - 2) se i servizi siano stati debitamente svolti;
  - 3) se ogni pagamento da effettuarsi al socio in affari sia ragionevole e proporzionato rispetto a tali servizi. Ciò è particolarmente importante onde evitare il rischio che il socio in affari utilizzi parte del pagamento ricevuto dall'organizzazione per pagare tangenti per conto o a vantaggio dell'organizzazione. Per esempio, se un agente è stato nominato dall'organizzazione per assistere le vendite ed è previsto che gli venga corrisposta una commissione o una provvigione previa aggiudicazione di un appalto all'organizzazione, l'organizzazione necessita di essere ragionevolmente soddisfatta del fatto che il pagamento della commissione sia ragionevole e proporzionato rispetto ai servizi legittimi effettivamente resi dall'agente, considerando il rischio assunto dall'agente nel caso in cui l'appalto non sia aggiudicato. Qualora sia corrisposta una commissione o una provvigione eccessivamente elevata, sussiste un rischio maggiore che parte di essa possa essere indebitamente utilizzata dall'agente per spingere un pubblico ufficiale o un impiegato del cliente dell'organizzazione ad aggiudicare l'appalto all'organizzazione. L'organizzazione può anche richiedere che i soci in affari forniscano la documentazione che comprova che i servizi siano stati forniti;
- c) aggiudicare appalti, laddove ciò sia possibile e ragionevole, solo dopo che si sia svolto un processo di bando di gara equo e, se del caso, trasparente tra almeno tre offerenti;
- d) richiedere che almeno due persone valutino le offerte e approvino l'aggiudicazione di un bando;
- e) attuare una separazione di compiti, in modo che i membri del personale che approvano l'aggiudicazione dell'appalto siano diversi rispetto a coloro che richiedono l'aggiudicazione dell'appalto e che siano di un reparto o di una funzione diversi da coloro che gestiscono l'appalto o approvano il lavoro svolto in base all'appalto;
- f) richiedere le firme di almeno due persone sui contratti e sui documenti che modificano le condizioni di un contratto o che approvano il lavoro svolto o le forniture previste dal contratto;
- g) porre un livello maggiore di supervisione da parte della direzione sulle transazioni a rischio di corruzione potenzialmente alto;
- h) proteggere l'integrità delle offerte e di altre informazioni legate ai prezzi limitando l'accesso solo alle persone competenti;
- i) fornire gli strumenti e gli schemi appropriati di supporto al personale (per esempio guide pratiche, comportamenti corretti ed errati, gerarchie per l'approvazione, liste di controllo, moduli, flusso di lavoro informatizzato).

Nota Ulteriori esempi di controlli e istruzioni sono forniti nella ISO 19600.

<i>revisione</i>	<i>data</i>	<i>emissione</i>	<i>approvazione</i>	<i>Pagina</i>
0	20/09/2018	RGQ	AU	20 di 28

## 8.13 Attuazione del sistema di gestione per la prevenzione della corruzione da parte di organizzazioni controllate e soci in affari

### 8.13.1 Generalità

**8.13.1.1** La ragione per i requisiti di cui al punto 8.5 della norma è che sia le organizzazioni controllate sia i soci in affari possono porre dei rischi di corruzione all'organizzazione. Le tipologie di rischi di corruzione che l'organizzazione punta a evitare in tali casi sono, per esempio, che:

- a) una sussidiaria dell'organizzazione paghi una tangente con il risultato che l'organizzazione ne possa rispondere;
- b) una joint venture o un partner di joint venture paghi una tangente per accaparrarsi del lavoro per una joint venture in cui partecipa l'organizzazione;
- c) un responsabile degli approvvigionamenti di un cliente o di un acquirente richieda una tangente all'organizzazione in cambio dell'aggiudicazione di un appalto;
- d) un cliente dell'organizzazione richieda all'organizzazione di nominare un sub-appaltatore o un fornitore specifico in circostanze in cui un manager del cliente o un pubblico ufficiale possa trarre personale beneficio da tale nomina;
- e) un agente dell'organizzazione paghi una tangente a un manager dell'acquirente dell'organizzazione per conto dell'organizzazione;
- f) un fornitore o un sub-fornitore dell'organizzazione paghi una tangente al responsabile degli approvvigionamenti dell'organizzazione in cambio dell'aggiudicazione di un appalto.

**8.13.1.2** Se l'organizzazione controllata o il socio in affari hanno attuato controlli per la prevenzione della corruzione rispetto a tali rischi, il conseguente rischio di corruzione dell'organizzazione normalmente è ridotto.

**8.13.1.3** Tale requisito di cui al punto 8.5 della norma distingue tra le organizzazioni su cui l'organizzazione detiene il controllo e quelle su cui non lo detiene. Ai fini del presente requisito, un'organizzazione detiene il controllo su un'altra organizzazione qualora controlli direttamente o indirettamente gli organi dirigenziali dell'organizzazione. Un'organizzazione potrebbe avere il controllo, per esempio, su una sussidiaria, una joint venture o un consorzio tramite la maggioranza dei voti in consiglio o tramite la maggioranza delle azioni. L'organizzazione non detiene il controllo su un'altra organizzazione ai fini del presente requisito solamente perché impiega una grande quantità di lavoro in tale altra organizzazione.

### 8.13.2 Organizzazioni controllate

**8.13.2.1** È ragionevole aspettarsi che l'organizzazione richieda che l'altra organizzazione, di cui ha il controllo, applichi controlli per la prevenzione della corruzione ragionevoli e proporzionati. Ciò potrebbe avvenire tramite l'attuazione da parte dell'organizzazione controllata del medesimo sistema di gestione per la prevenzione della corruzione come applicato dall'organizzazione stessa, oppure tramite l'attuazione da parte dell'organizzazione controllata dei propri controlli specifici per la prevenzione della corruzione. Tali controlli dovrebbero essere ragionevoli e proporzionati rispetto ai rischi di corruzione a cui l'organizzazione controllata è sottoposta, prendendo in considerazione la valutazione del rischio di corruzione condotta in conformità al punto 4.5 della norma.

**8.13.2.2** Laddove un socio in affari sia controllato dall'organizzazione (per esempio in una joint venture su cui l'organizzazione detiene il controllo di gestione), tale socio in affari controllato ricadrebbe nei requisiti di cui al punto 8.5.1 della norma.

### 8.13.3 Soci in affari non controllati

**8.13.3.1** Per quanto concerne i soci in affari che non sono controllati dall'organizzazione, l'organizzazione può non dover adottare nessuna misura richiesta dal punto 8.5.2 della norma per richiedere l'attuazione da parte del socio in affari di controlli per la prevenzione della corruzione nelle seguenti circostanze:

- a) laddove il socio in affari non ponga rischio di corruzione o ponga un rischio di corruzione basso;
- b) laddove il socio in affari ponga un rischio di corruzione superiore al livello basso, ma i controlli che potrebbero essere applicati da parte del socio in affari non aiuterebbero a limitare il rischio in questione (non avrebbe senso insistere affinché il socio in affari applicasse tali controlli che non servirebbero; tuttavia, in tal caso, ci si aspetterebbe che l'organizzazione prendesse tale fattore in considerazione nella propria valutazione del rischio al fine di informare i decisori rispetto all'eventualità di procedere e in quale modo in tale relazione).

Ciò rispecchia i concetti di ragionevolezza e proporzionalità della norma.

**8.13.3.2** Qualora la valutazione del rischio di corruzione (vedere punto 4.5 della norma) o la due diligence (vedere punto 8.2 della norma) giunga alla conclusione che un socio in affari non controllato pone più di un

<i>revisione</i>	<i>data</i>	<i>emissione</i>	<i>approvazione</i>	<i>Pagina</i>
0	20/09/2018	RGQ	AU	21 di 28

rischio basso di corruzione e che i controlli per la prevenzione della corruzione attuati dal socio in affari contribuirebbero a limitare tale rischio di corruzione, l'organizzazione dovrebbe adottare le seguenti misure aggiuntive in base al punto 8.5 della ISO 37001.

a) L'organizzazione determina se il socio in affari mette in atto controlli adeguati per la prevenzione della corruzione che affrontano il rischio di corruzione in questione.

L'organizzazione dovrebbe effettuare tale valutazione dopo aver eseguito una due diligence appropriata (v. §8.10). L'organizzazione sta cercando di verificare che tali controlli affrontino il rischio di corruzione riguardante la transazione tra l'organizzazione e il socio in affari. L'organizzazione non è tenuta a verificare che il socio in affari detenga il controllo sui propri rischi di corruzione più ampi. Si noti che sia l'entità dei controlli sia le misure che l'organizzazione deve adottare per verificare tali controlli dovrebbero essere ragionevoli e proporzionati al rischio di corruzione in questione. Se l'organizzazione ha determinato per quanto possa ragionevolmente fare che il socio in affari ha in essere controlli adeguati, il requisito di cui al requisito 8.5 della norma è trattato nei confronti di tale socio in affari. Vedere § 8.13.3.4 per i commenti sui tipi di controlli adeguati.

b) Qualora l'organizzazione rilevi che il socio in affari non abbia in essere controlli per la prevenzione della corruzione adeguati che affrontino i rischi di corruzione pertinenti, o qualora non sia possibile verificare se abbia in essere tali controlli, l'organizzazione adotta le seguenti misure aggiuntive.

1) Se fattibile (vedere §8.13.3.3), l'organizzazione richiede che il socio in affari dia attuazione ai controlli per la prevenzione della corruzione (vedere §8.13.3.4) in riferimento alla transazione, al progetto o all'attività pertinente.

2) Laddove non sia fattibile (vedere §8.13.3.3) richiedere al socio in affari di attuare i controlli per la prevenzione della corruzione, l'organizzazione prende in considerazione tale fattore durante la valutazione dei rischi di corruzione che il socio in affari pone e il modo in cui l'organizzazione gestisce tali rischi. Ciò non significa che l'organizzazione non possa procedere nella relazione o nella transazione. Tuttavia, l'organizzazione dovrebbe ponderare, nell'ambito della valutazione del rischio di corruzione, l'eventualità che il socio in affari sia coinvolto in atti di corruzione e l'organizzazione dovrebbe prendere in considerazione l'assenza di tali controlli quando valuta il rischio complessivo di corruzione. Se l'organizzazione ritiene che i rischi di corruzione posti da tale socio in affari siano inaccettabilmente alti e che il rischio di corruzione non possa essere ridotto in altro modo (per esempio rivedendo la transazione), si applicano le disposizioni di cui al punto 8.8 della norma.

**8.13.3.3** La fattibilità per l'organizzazione di richiedere a un socio in affari non controllato di attuare i controlli dipende dalle circostanze. Per esempio:

a) Normalmente ciò è fattibile quando l'organizzazione ha un grado significativo di influenza sul socio in affari. Per esempio, quando l'organizzazione nomina un agente affinché agisca per suo conto in una transazione oppure nomina un sub-appaltatore con un ampio campo di lavoro. In questo caso, l'organizzazione solitamente è in grado di mettere l'attuazione dei controlli per la prevenzione della corruzione come condizione di tale nomina.

b) Normalmente ciò non è fattibile quando l'organizzazione non ha un grado significativo di influenza sul socio in affari, per esempio:

1) un cliente per un progetto;

2) un sub-appaltatore o fornitore specifico nominato dal cliente;

3) un principale sub-appaltatore o fornitore quando il potere di contrattazione del fornitore o del sub-appaltatore è di gran lunga maggiore rispetto a quello dell'organizzazione (per esempio quando l'organizzazione acquisita componenti da un fornitore principale in base alle condizioni standard del fornitore).

c) Normalmente non è fattibile quando il socio in affari non dispone delle risorse o delle competenze per poter attuare i controlli.

**8.13.3.4** I tipi di controlli richiesti dall'organizzazione dipendono dalle circostanze. Essi dovrebbero essere ragionevoli e proporzionati al rischio di corruzione e, come minimo, dovrebbero comprendere il rischio di corruzione pertinente nell'ambito del loro campo di applicazione. A seconda della natura del socio in affari e della natura del rischio di corruzione che pone, l'organizzazione ha facoltà, per esempio, di adottare le seguenti misure.

a) In caso di un socio in affari ad alto rischio di corruzione con un campo di lavoro ampio e complesso, l'organizzazione potrebbe richiedere al socio in affari di attuare controlli equivalenti a quelli previsti dal presente documento rispetto ai rischi di corruzione che pone all'organizzazione.

<i>revisione</i>	<i>data</i>	<i>emissione</i>	<i>approvazione</i>	<i>Pagina</i>
0	20/09/2018	RGQ	AU	22 di 28

b) In caso di un socio in affari di medie dimensioni con un rischio di corruzione medio, l'organizzazione può richiedere che il socio in affari applichi alcuni requisiti minimi per la prevenzione della corruzione in relazione alla transazione, per esempio una politica per la prevenzione della corruzione, formazione per i propri impiegati interessati, un manager responsabile per la conformità riguardo la transazione, controlli sui pagamenti chiave e una linea per le segnalazioni.

c) In caso di un socio in affari di modeste dimensioni che ha un campo di lavoro molto specifico (per esempio un agente o un fornitore secondario), l'organizzazione ha facoltà di richiedere una formazione per gli impiegati interessati e controlli sui pagamenti chiave, sui regali e sull'ospitalità.

Tali controlli devono funzionare in relazione alla transazione tra l'organizzazione e il socio in affari (sebbene in pratica il socio in affari abbia facoltà di avere controlli in essere riguardanti le proprie attività commerciali nel loro complesso).

Quanto di cui sopra è meramente a titolo di esempio. La questione fondamentale è che l'organizzazione identifichi i rischi chiave di corruzione legati alla transazione e richieda, per quanto fattibile, che il socio in affari attui controlli ragionevoli e proporzionati su tali rischi chiave di corruzione.

**8.13.3.5** L'organizzazione in genere impone tali requisiti sui soci in affari non controllati quali preconditione per collaborare con il socio in affari e/o inserendoli nella documentazione contrattuale.

**8.13.3.6** L'organizzazione non è tenuta a verificare la completa conformità a tali requisiti da parte del socio in affari non controllato. Tuttavia, l'organizzazione dovrebbe adottare le misure ragionevoli per assicurarsi che il socio in affari li osservi (per esempio richiedendo al socio in affari di fornire le copie dei propri documenti rilevanti sulla politica). In casi di rischi elevati di corruzione (per esempio di un agente), l'organizzazione può attuare procedure di monitoraggio, segnalazione e/o audit.

**8.13.3.7** Visto che l'attuazione dei controlli per la prevenzione della corruzione può richiedere tempo, è probabile che sia ragionevole che un'organizzazione fornisca ai propri soci in affari il tempo per applicare tali controlli. L'organizzazione potrebbe continuare a lavorare con tale socio in affari ad interim, ma l'assenza di tali controlli rappresenterebbe un fattore nella valutazione del rischio e nella due diligence effettuate. Ciononostante, l'organizzazione dovrebbe valutare di richiedere il diritto di risolvere il contratto o l'accordo pertinente qualora il socio in affari non attui efficacemente i controlli richiesti in modo tempestivo.

## 8.14 Impegni per la prevenzione della corruzione

**8.14.1** Il presente requisito volto a ottenere impegni per la prevenzione della corruzione si applica solo ai soci in affari che pongono un rischio di corruzione superiore allivello basso.

**8.14.2** È probabile che il rischio di corruzione legato a una transazione sia basso, per esempio:

- quando l'organizzazione acquista un numero modesto di articoli di valore molto basso;
- quando l'organizzazione prenota voli aerei o stanze in albergo online direttamente dalle compagnie aeree o dagli alberghi;
- quando l'organizzazione fornisce beni o servizi di basso valore direttamente all'acquirente (per esempio generi alimentari, biglietti per il cinema).

In questi casi, l'organizzazione non dovrebbe richiedere di ottenere impegni per la prevenzione della corruzione da tali fornitori o acquirenti a basso rischio di corruzione.

**8.14.3** Nel caso di un socio in affari che pone un rischio di corruzione superiore al livello basso, l'organizzazione dovrebbe, se fattibile, ottenere impegni per la prevenzione della corruzione da tale socio in affari.

a) Normalmente è fattibile richiedere tali impegni quando l'organizzazione ha influenza sul socio in affari e può insistere affinché il socio in affari conceda tali impegni. È probabile che l'organizzazione sia in grado di richiedere tali impegni, per esempio, quando l'organizzazione nomina un agente affinché agisca per suo conto in una transazione oppure nomina un subappaltatore con un ampio campo di lavoro.

b) Può darsi che l'organizzazione non abbia sufficiente influenza da essere in grado di richiedere tali impegni in relazione, per esempio, ad affari con clienti o acquirenti principali, oppure quando l'organizzazione acquista componenti da un fornitore principale alle condizioni standard del fornitore. In questi casi, l'assenza di tali disposizioni non significa che il progetto o la relazione non debba proseguire, ma l'assenza di tale impegno dovrebbe essere considerata come fattore rilevante nella valutazione del rischio di corruzione e durante la due diligence effettuata in base ai punti 4.5 e 8.2 della norma.

**8.14.4** Tali impegni dovrebbero, per quanto possibile, essere ottenuti in forma scritta. Ciò potrebbe avvenire o con un documento di impegni separato o inserendoli in un contratto tra l'organizzazione e il socio in affari.

<i>revisione</i>	<i>data</i>	<i>emissione</i>	<i>approvazione</i>	<i>Pagina</i>
0	20/09/2018	RGQ	AU	23 di 28

### 8.15 Regali, ospitalità, donazioni e benefici simili

**8.15.1** L'organizzazione deve essere consapevole che i regali, l'ospitalità, le donazioni e gli altri benefici possono essere percepiti da una parte terza (per esempio da un concorrente in affari, dalla stampa, da un pubblico ministero o un giudice) di avere lo scopo di corrompere anche se ciò non era l'intento né del donatore né del beneficiario. Un utile meccanismo di controllo è evitare per quanto possibile qualsivoglia regalo, atto di ospitalità, donazione e altri benefici che potrebbero essere ragionevolmente essere percepiti da una parte terza di avere lo scopo di corrompere.

**8.15.2** I benefici di cui al punto 8.7 della norma potrebbero comprendere, per esempio:

- a) regali, intrattenimento e ospitalità;
- b) donazioni a enti politici o benefici;
- c) viaggi per rappresentanti del cliente o pubblici ufficiali;
- d) spese promozionali;
- e) sponsorizzazioni;
- f) benefici per la comunità;
- g) formazione;
- h) iscrizioni a circoli privati;
- i) favori personali;
- j) informazioni riservate e privilegiate.

**8.15.3** Per quanto riguarda i regali e l'ospitalità, le procedure attuate dall'organizzazione potrebbero, per esempio, essere progettate per:

- a) controllare l'entità e la frequenza di regali e ospitalità tramite:
  - 1) un divieto assoluto di fare regali e offrire ospitalità;
  - 2) il permesso di fare regali e offrire ospitalità ma limitandoli, come riferimento, a fattori come:
    - i) una spesa massima (che può variare secondo il luogo e il tipo di regali e ospitalità);
    - ii) la frequenza (regali e ospitalità relativamente di basso valore se ripetuti possono formare complessivamente un valore elevato);
    - iii) tempistiche (per esempio non durante o immediatamente prima o dopo trattative per appalti);
    - iv) ragionevolezza (considerando il luogo, il settore e l'anzianità del donatore o del beneficiario);
    - v) l'identità del beneficiario (per esempio coloro nella posizione di poter aggiudicare gli appalti o approvare i permessi, i certificati o i pagamenti);
    - vi) reciprocità (nessuno nell'organizzazione può ricevere regali o ospitalità di valore superiore a quello che possono dare);
    - vii) l'ambiente giuridico e normativa (alcuni luoghi e organizzazioni possono avere dei divieti o controlli in essere).
- b) richiedere un'approvazione anticipata dei regali e dell'ospitalità al di sopra di un valore o di una frequenza prestabiliti da un dirigente competente;
- c) richiedere che i regali e l'ospitalità al di sopra di un valore prestabilito avvengano in modo trasparente, che siano documentati con efficacia (per esempio in un registro o libro contabile) e siano supervisionati.

**8.15.4** Per quanto riguarda le donazioni a enti politici o benefici, le sponsorizzazioni, le spese promozionali e i benefici per la comunità, le procedure attuate dall'organizzazione potrebbero, per esempio, essere progettate per:

- a) vietare i pagamenti volti a influenzare, o che potrebbero ragionevolmente essere percepiti con la finalità di influenzare, un bando o un'altra decisione a favore dell'organizzazione;
- b) effettuare la due diligence sul partito politico, sull'ente benefico o su altri beneficiari per stabilire se siano legittimi e che non siano utilizzati come canale di corruzione (per esempio ciò potrebbe comprendere ricerche in rete o altre richieste per determinare se i dirigenti del partito politico o dell'ente benefico abbiano una reputazione di corruzione o comportamenti illeciti simili, oppure se siano collegati ai progetti o agli acquirenti dell'organizzazione);
- c) richiedere che un manager competente approvi il pagamento;
- d) richiedere la divulgazione pubblica del pagamento;
- e) garantire che il pagamento sia lecito dalle leggi e dalle regolamentazioni vigenti;
- f) evitare di dare contributi immediatamente prima, durante o immediatamente dopo trattative contrattuali.

**8.15.5** Per quanto riguarda i viaggi di rappresentanti del cliente o di pubblici ufficiali, le procedure attuate dall'organizzazione potrebbero, per esempio, essere progettate per:

<i>revisione</i>	<i>data</i>	<i>emissione</i>	<i>approvazione</i>	<i>Pagina</i>
0	20/09/2018	RGQ	AU	24 di 28

- a) consentire solo i pagamenti che sono permessi dalle procedure del cliente o dell'ente pubblico e dalle leggi e regolamentazioni vigenti;
- b) consentire solo i viaggi necessari per il corretto svolgimento dei compiti del rappresentante del cliente o del pubblico ufficiale (per esempio per ispezionare le procedure di qualità dell'organizzazione presso il proprio stabilimento);
- c) richiedere che un manager competente dell'organizzazione approvi il pagamento;
- d) richiedere, se possibile, che il supervisore o il datore di lavoro o la funzione di conformità per la prevenzione della corruzione del pubblico ufficiale sia messo a conoscenza del viaggio e dell'ospitalità in programma;
- e) limitare i pagamenti al viaggio, all'alloggio e alle spese per i pasti indispensabili e direttamente collegate a un itinerario di viaggio ragionevole;
- f) limitare le occasioni di intrattenimento associato a un livello ragionevole rispetto alla politica sui regali e sull'ospitalità dell'organizzazione;
- g) vietare il pagamento delle spese a famigliari o amici;
- h) vietare il pagamento di vacanze o spese per svago.

### 8.16 Audit interno

**8.16.1** Il requisito di cui al punto 9.2 della norma non significa che un'organizzazione sia obbligata ad avere la propria funzione separata di audit interno. Dispone che l'organizzazione nomini una funzione idonea, competente e indipendente oppure una persona con la responsabilità di effettuare tale audit. Un'organizzazione ha facoltà di utilizzare una parte terza affinché gestisca il proprio programma di audit interno oppure ha facoltà di incaricare una parte terza affinché attui determinate parti di un programma esistente.

**8.16.2** La frequenza dell'audit dipende dai requisiti dell'organizzazione. È probabile che alcuni progetti, procedure, controlli e sistemi siano selezionati a campione da sottoporre a audit ogni anno.

**8.16.3** La selezione del campione può basarsi sul rischio, in modo che, per esempio, un progetto a elevato rischio di corruzione sia selezionato per un audit antepoendolo per priorità a un progetto a basso rischio di corruzione.

**8.16.4** Normalmente gli audit devono essere programmati in anticipo in modo che le parti interessate abbiano a disposizione i documenti e il tempo necessari. Tuttavia, in alcuni casi, l'organizzazione può ritenere utile effettuare un audit che le parti sottoposte ad audit non si aspettano.

**8.16.5** Se un'organizzazione possiede un organo direttivo, tale organo direttivo ha facoltà anche di gestire la scelta e la frequenza degli audit dell'organizzazione in base a quel che reputa necessario, al fine di esercitare la propria indipendenza e di contribuire a garantire che gli audit siano indirizzati alle aree dell'organizzazione a rischio di corruzione primario. L'organo direttivo ha altresì facoltà di richiedere l'accesso a tutti i verbali e i risultati dell'audit e di richiedere che gli audit correlati a certi tipi di questioni a rischio di corruzione più elevato o a certi tipi di indicatori di rischio siano riferiti all'organo direttivo una volta che l'audit si è concluso.

**8.16.6** L'intento dell'audit è fornire una ragionevole certezza all'organo direttivo (se presente) e all'alta direzione che il sistema di gestione per la prevenzione della corruzione sia stato applicato e che stia funzionando in modo efficace, al fine di contribuire a prevenire e rilevare atti di corruzione, nonché di fungere da deterrente per eventuali membri corrotti del personale (dal momento che sarebbero consapevoli che il loro progetto o il loro reparto potrebbe essere scelto per un audit).

### 8.17 Informazioni documentate

Le informazioni documentate in base al punto 7.5.1 della norma possono includere:

- a) la ricezione della politica per la prevenzione della corruzione da parte del personale;
- b) la fornitura della politica per la prevenzione della corruzione ai soci in affari che pongono un rischio di corruzione superiore al livello basso;
- c) le politiche, le procedure e i controlli del sistema di gestione per la prevenzione della corruzione;
- d) i risultati della valutazione del rischio di corruzione (vedere punto 4.5 della norma);
- e) la formazione fornita per la prevenzione della corruzione (vedere punto 7.3 della ISO 37001);
- f) la due diligence effettuata;
- g) le misure adottate per attuare il sistema di gestione per la prevenzione della corruzione;
- h) le approvazioni e le registrazioni di regali, ospitalità, donazioni e benefici simili forniti e ricevuti (vedere punto 8.7 dello standard);
- i) le azioni e gli esiti dei sospetti sollevati in merito a:

<i>revisione</i>	<i>data</i>	<i>emissione</i>	<i>approvazione</i>	<i>Pagina</i>
0	20/09/2018	RGQ	AU	25 di 28

- 1) qualsivoglia debolezza del sistema per la prevenzione della corruzione;
  - 2) episodi di corruzione tentati, sospetti o effettivi;
- j) i risultati del monitoraggio, delle indagini o degli audit effettuati da parte dell'organizzazione o di parti terze.

## 8.18 Indagini e gestione della corruzione

### 8.18.1

La ISO 37001 prevede che l'organizzazione attui procedure adeguate relative a come indagare e affrontare qualsiasi caso di corruzione o inadempimento dei controlli per la prevenzione della corruzione che siano riferiti, rilevati o ragionevolmente presunti. Il modo in cui un'organizzazione indaga e affronta i casi particolari dipende dalle circostanze. Ogni situazione è diversa e la risposta dell'organizzazione dovrebbe essere ragionevole e proporzionata alle circostanze. Una segnalazione di un caso grave di presunta corruzione prevedrebbe un'azione molto più urgente, significativa e dettagliata rispetto a un inadempimento minore ai controlli per la prevenzione della corruzione. Le proposte qui sotto sono a mero titolo di guida e non devono essere considerate in ottica prescrittiva.

**8.18.2** La funzione di conformità dovrebbe preferibilmente essere il destinatario di qualsivoglia segnalazione di atti di corruzione o inadempimenti effettivi o presunti. Qualora le segnalazioni siano rivolte in prima istanza a un'altra persona, le procedure dell'organizzazione dovrebbero prevedere che la segnalazione sia inoltrata alla funzione di conformità quanto prima. In alcuni casi, la funzione di conformità identifica a propria volta un sospetto o un inadempimento.

**8.18.3** La procedura dovrebbe determinare chi ha la responsabilità di decidere il modo in cui indagare e affrontare la questione. Per esempio:

- a) un'organizzazione di modeste dimensioni ha facoltà di adottare una procedura in base alla quale tutte le questioni, indipendentemente dalla loro entità, dovrebbero essere riferite immediatamente da parte della funzione di conformità all'alta direzione affinché essa decida il modo di affrontarla;
- b) un'organizzazione di più grandi dimensioni ha facoltà di adottare una procedura in base alla quale:
  - 1) le questioni minori sono affrontate dalla funzione di conformità, sottoponendo all'alta direzione una relazione di sintesi periodica di tutte le questioni minori;
  - 2) le questioni più gravi sono riferite immediatamente da parte della funzione di conformità all'alta direzione affinché essa decida il modo di affrontarla.

**8.18.4** Per qualsiasi questione rilevata, l'alta direzione o la funzione di conformità (se del caso) dovrebbe valutare i fatti noti e la potenziale gravità della questione. Qualora essi non possedessero già fatti a sufficienza su cui prendere una decisione, dovrebbero avviare un'indagine.

**8.18.5** L'indagine dovrebbe essere svolta da una persona estranea alla questione. Potrebbe essere la funzione di conformità, l'auditor interno, un altro manager competente o una parte terza competente. La persona che svolge l'indagine dovrebbe ricevere da parte dell'alta direzione l'autorità, le risorse e l'accesso adeguati per consentire che l'indagine sia condotta con efficacia. La persona che svolge l'indagine dovrebbe preferibilmente avere conseguito una formazione o avere esperienza pregressa nella conduzione di indagini. L'indagine dovrebbe accertare tempestivamente i fatti e raccogliere tutte le prove necessarie, per esempio:

- a) svolgendo interrogazioni per determinare i fatti;
- b) raccogliendo tutti i documenti pertinenti e le altre prove;
- c) ottenendo testimonianze;
- d) laddove possibile e ragionevole, richiedendo che siano stilati rapporti per iscritto e che siano sottoscritte dagli individui che le rilasciano.

**8.18.6** Nello svolgimento di un'indagine e di qualsiasi azione successiva, l'organizzazione deve ponderare i fattori rilevanti, per esempio:

- a) le leggi vigenti (potrebbe servire ricorrere a una consulenza legale);
- b) la sicurezza del personale;
- c) il rischio di diffamazione nel rilasciare dichiarazioni;
- d) la tutela delle persone che fanno segnalazioni e di altri coinvolti o menzionati nella segnalazione (vedere punto 8.9 della norma);
- e) potenziali responsabilità penali, civili e amministrative, perdite finanziarie e danni alla reputazione per l'organizzazione e gli individui;
- f) qualunque obbligo giuridico o beneficio per l'organizzazione da segnalare alle autorità;
- g) il mantenimento del segreto sulla questione e sull'indagine finché non si siano accertati i fatti;

<i>revisione</i>	<i>data</i>	<i>emissione</i>	<i>approvazione</i>	<i>Pagina</i>
0	20/09/2018	RGQ	AU	26 di 28

h) la necessità dell'alta direzione di richiedere la piena collaborazione da parte dei membri del personale coinvolti nell'indagine.

**8.18.7** Risultati dell'indagine dovrebbero essere riferiti all'alta direzione o alla funzione di conformità come opportuno. Se i risultati sono riferiti all'alta direzione, dovrebbero essere comunicati anche alla funzione di conformità per la prevenzione della corruzione.

**8.18.8** Una volta che l'organizzazione ha terminato l'indagine e/o ha informazioni sufficienti per essere in grado di prendere una decisione, l'organizzazione dovrebbe attuare azioni conseguenti appropriate. A seconda delle circostanze e della gravità della questione, esse potrebbero comprendere una o più fra le seguenti azioni:

- a) risolvere, ritirare o modificare il coinvolgimento dell'organizzazione nel progetto, nella transazione o nel contratto;
- b) restituire o richiedere la restituzione di qualsiasi beneficio improprio;
- c) assumere misure disciplinari nei confronti dei membri del personale coinvolti (che, in base alla gravità della questione, potrebbero andare da un richiamo per una violazione secondaria al licenziamento per una violazione grave);
- d) denunciare la questione alle autorità;
- e) nel caso si siano verificati atti di corruzione, adottare azioni per evitare o affrontare qualsiasi possibile violazione giuridica conseguente (per esempio, un errore in bilancio che può verificarsi laddove una tangente venga impropriamente registrata nella contabilità, una violazione fiscale nel caso in cui una tangente sia illecitamente dedotta dal reddito oppure riciclaggio di denaro sporco nel caso si tratti di proventi risultanti da un reato).

**8.18.9** L'organizzazione dovrebbe sottoporre a riesame le procedure di prevenzione della corruzione per esaminare se la questione sia scaturita da una qualche inadeguatezza delle procedure e, se fosse questo il caso, dovrebbe adottare misure immediate e adeguate per migliorare tali procedure.

## 8.19 Monitoraggio

Il monitoraggio del sistema di gestione per la prevenzione della corruzione può includere, per esempio, gli ambiti seguenti:

- a) l'efficacia della formazione;
- b) l'efficacia dei controlli, per esempio mediante gli esiti di prove campione;
- c) l'efficacia della distribuzione delle responsabilità per soddisfare i requisiti del sistema di gestione per la prevenzione della corruzione;
- d) l'efficacia nel rispondere a insuccessi relativi alla conformità precedentemente identificati;
- e) i casi nei quali gli audit interni di conformità non sono eseguiti come programmato.

Il monitoraggio della prestazione di conformità può includere, per esempio, gli ambiti seguenti:

- le non conformità e i "near misses" (ossia gli incidenti senza effetti negativi);
- i casi nei quali i requisiti per la prevenzione della corruzione non sono rispettati;
- i casi nei quali gli obiettivi non sono raggiunti;
- lo stato della cultura della conformità.

Nota. Vedere ISO 19600.

L'organizzazione può periodicamente eseguire auto-valutazioni, su tutta l'organizzazione o su parti di essa, al fine di valutare l'efficacia del sistema di gestione per la prevenzione della corruzione (vedere punto 9.4 della norma).

## 8.20 Programmazione e attuazione di modifiche al sistema di gestione per la prevenzione della corruzione

**8.20.1** L'adeguatezza e l'efficacia del sistema di gestione per la prevenzione della corruzione dovrebbero essere valutate su base continua e regolare attraverso vari metodi, per esempio riesami tramite audit interni, della direzione e della funzione di conformità per la prevenzione della corruzione (vedere il punto 9.4 della norma).

**8.20.2** L'organizzazione dovrebbe considerare i risultati e gli esiti di tali valutazioni per stabilire se ci sia l'esigenza o l'opportunità di modificare il sistema di gestione per la prevenzione della corruzione.

**8.20.3** Al fine di contribuire a garantire l'integrità del sistema di gestione per la prevenzione della corruzione e di mantenerne l'efficacia, le modifiche a singoli elementi del sistema di gestione dovrebbero tenere in

<i>revisione</i>	<i>data</i>	<i>emissione</i>	<i>approvazione</i>	<i>Pagina</i>
0	20/09/2018	RGQ	AU	27 di 28

considerazione la dipendenza e l'impatto di tali modifiche sull'efficacia del sistema di gestione per la prevenzione della corruzione nel suo complesso.

**8.20.4** Quando l'organizzazione stabilisce l'esigenza di apportare cambiamenti al sistema di gestione per la prevenzione della corruzione, tali cambiamenti dovrebbero essere svolti in modo programmato considerando quanto segue:

- a) lo scopo dei cambiamenti e le loro potenziali conseguenze;
- b) l'integrità del sistema per la prevenzione della corruzione;
- c) la disponibilità di risorse;
- d) la distribuzione o ridistribuzione di responsabilità e autorità;
- e) la velocità, l'entità e l'arco temporale dell'attuazione delle modifiche.

**8.20.5** I potenziamenti del sistema di gestione per la prevenzione della corruzione in conseguenza alle misure adottate in seguito a non conformità e risultanti dai miglioramenti continui (vedere punto 10 della norma) dovrebbero essere eseguiti in base al medesimo approccio di cui al §8.20.4 del presente documento.

### 8.21 Pubblici ufficiali

Il termine "pubblico ufficiale" (cfr. punto 3.27 della norma) è definito in molte leggi per la prevenzione della corruzione.

La lista seguente non è esauriente e non tutti gli esempi si applicano a ogni giurisdizione. Nella valutazione dei rischi di corruzione, un'organizzazione dovrebbe prendere in considerazione le categorie di pubblici ufficiali con cui può ritrovarsi ad avere a che fare.

Il termine "pubblico ufficiale" può comprendere quanto segue:

- a) un titolare di pubblico ufficio a livello nazionale, statale, provinciale o comunale, compresi i membri degli organi legislativi, chi detiene poteri esecutivi e la magistratura;
- b) funzionari di partiti politici;
- c) i candidati a pubblici uffici;
- d) i dipendenti pubblici, compresi i dipendenti dei ministeri, delle agenzie governative, dei tribunali amministrativi e degli enti pubblici;
- e) i funzionari delle organizzazioni internazionali pubbliche, per esempio la Banca Mondiale, le Nazioni Unite o il Fondo Monetario Internazionale;
- f) i dipendenti di imprese controllate dal pubblico, a meno che l'impresa non operi su normale base commerciale nel mercato di riferimento, ossia su una base sostanzialmente equivalente a quella di un'impresa privata, senza sussidi preferenziali o altri privilegi.

In molte giurisdizioni, anche i parenti e gli stretti collaboratori dei pubblici ufficiali sono considerati essere pubblici ufficiali ai fini delle leggi per la prevenzione della corruzione.

### 8.22 Iniziative per la prevenzione della corruzione

Sebbene non si tratti di un requisito della norma, l'organizzazione può ritenere utile condividere o valutare le raccomandazioni di qualsiasi iniziativa settoriale o altre iniziative per la prevenzione della corruzione che promuovono o pubblicano buone pratiche per la prevenzione della corruzione pertinenti alle attività dell'organizzazione.

<i>revisione</i>	<i>data</i>	<i>emissione</i>	<i>approvazione</i>	<i>Pagina</i>
0	20/09/2018	RGQ	AU	28 di 28