PROCEDURA E REGISTRAZIONI DI DUE DILIGENCE – REQUISITO 8.2 ISO 37001

UNI ISO 37001:2016 – COSBOTEK S.r.l.

1. Scopo e campo di applicazione

La presente procedura disciplina la due diligence (DD) anticorruzione su progetti, transazioni e personale in coerenza con il requisito 8.2 della ISO 37001. È applicata a: (i) nuove commesse/progetti e variazioni rilevanti; (ii) transazioni economico-finanziarie non ordinarie o a maggior esposizione; (iii) soci in affari (fornitori, consulenti, subappaltatori, partner); (iv) personale destinato a ruoli esposti al rischio.

2. Riferimenti, ruoli e responsabilità

Riferimenti: UNI ISO 37001 §8.2; Modello 231 (Protocolli Gare/Acquisti/Finanza); PTPC (ove applicabile); D.Lgs. 24/2023 (WB); GDPR. Ruoli principali: Direzione (approvazioni di alto livello); Compliance Officer/RSGA (coordinamento e decisioni su risk rating e misure); Ufficio Gare/Commerciale (DD progetti); Acquisti (DD soci in affari); Amministrazione/Finanza (DD transazioni); HR (DD personale); OdV (vigilanza).

3. Approccio risk-based: livelli, criteri e frequenza

Livello rischio (residuo)	Esempi criteri di rischio	Profondità due diligence	Frequenza/Trigger	Approvazione richiesta	Evidenze minime
Basso	Cliente/fornitore UE con storia positiva; importi limitati; nessun contatto PA	DD semplificata (questionario etico; autocertificazioni; verifica liste interne)	All'ingresso; rinnovo biennale	Process Owner + Compliance	Questionario; visure base; verifica conflitti
Medio	Importi significativi; nuovi mercati; subappalto; interazioni PA indirette	DD standard (visure camerali complete; referenze; verifica PEP/sanzioni; analisi reputazionale open-source)	All'ingresso; rinnovo annuale; on event (variazioni rilevanti)	Compliance + Direzione/owner	Dossier DD firmato; check-list; esito risk rating
Alto	Paesi/settori ad alto rischio; forte interazione PA; consulenti interposti; pagamenti atipici	DD rafforzata (PEP/blacklist/sanzioni; beneficial ownership; struttura pagamenti; site visit; intervista; clausole rinforzate)	All'ingresso; riesame semestrale; obbligatorio on event	Direzione + Compliance; parere OdV	Report approfondito; delibera; piani di mitigazione

4. Due diligence su Progetti/Commesse

Ogni nuova commessa o variazione >10% valore/ambito è soggetta a DD proporzionata al rischio (cliente, territorio, valore, PA coinvolta, uso di intermediari). Red flags: richieste di intermediari non giustificati, pagamenti in contanti, urgenze immotivate, varianti frequenti.

Passo	Attività	Responsabile	Output/Evidenza	Livello DD	Esito/Decisione
Screening iniziale	Scheda commessa + scoring rischio (cliente/valore/PA/Paese)	Ufficio Gare	Scheda rischio	Semplificata/Std/Raff.	Idoneo/Non idoneo/mitigazioni
Raccolta info	Documenti cliente; contratto; eventuali partner/subappalti; flussi economici	Gare + Compliance	Dossier DD commessa	Std/Raff.	OK/OK con condizioni
Valutazione e piani	Analisi red flags; definizione misure (clausole, tracciabilità, doppie firme)	Compliance	Report DD	Std/Raff.	Delibera Direzione
Riesame on event	Aggiornamento su varianti/claim/fusioni cliente	Gare + Compliance	Addendum DD	Come da rischio	Conferma/Stop

5. Due diligence su Transazioni

Le transazioni straordinarie o atipiche (anticipi elevati, bonus di successo, consulenze, sponsorizzazioni, donazioni, pagamenti a terzi) richiedono DD proporzionata. È vietato l'uso di pagamenti a soggetti non parte del contratto senza approvazione.

Tipo transazione	Rischi tipici	Controlli/DD richiesti	Soglie/Frequenza	Approvazione	Registrazioni
Consulenze/Intermediari	Interposizione; success fee	Contratto dettagliato; verifica indipendenza/PEP; tariffario congruo	Sempre; riesame annuale	Direzione + Compliance	Contratto; due diligence; timesheet
Sponsorizzazioni/Donazioni	Schermo per utilità indebite	Coerenza con policy; beneficiario legittimo; tracciabilità; no PA salvo policy	On request; rinnovo annuale	Direzione	Delibera; ricevute; evidenze evento
Pagamenti anticipati/atipici	Sviamento fondi; conti non ufficiali	Doppia firma; IBAN verificato; match contratto/PO	Sempre > soglia	Amministrazione + Direzione	Check-list pagamento; estratti conto

6. Due diligence su Personale (assunzioni/cambi ruolo)

Per ruoli esposti (gare, acquisti, finanza, relazioni PA, capicantiere) è richiesta DD proporzionata: verifica referenze, autodichiarazioni conflitti, eventuale verifica PEP/sanzioni nei limiti di legge; formazione obbligatoria e firma Codice Etico.

Evento	Attività DD	Responsabile	Livello DD	Tempistica	Evidenze
Nuova assunzione (ruolo a rischio)	CV + referenze; conflitti; eventuale PEP/sanzioni; formazione onboarding	HR + Compliance	Std/Raff.	Prima dell'inserimento	Checklist DD HR; attestati
Cambio mansione (ruolo a rischio)	Re-assessment integrità; profili accesso IT; aggiornamento deleghe	HR + IT + RSGA	Sempl./Std.	Prima del cambio	Modulo cambio ruolo; log accessi
Rotazione/Segregazione	Piano rotazione; doppio controllo; limitazione poteri	Direzione + RSGA	Come da rischio	Annuale o su evento	Registro rotazioni; delibera

7. Workflow decisionale, escalation e clausole

Esiti DD: (A) Idoneo; (B) Idoneo con condizioni (clausole anticorruzione rinforzate, audit, doppia firma); (C) Non idoneo/Stop. Escalation: in presenza di red flags gravi, sospensione attività e decisione Direzione con parere OdV. Clausole minime: dichiarazione integrità, diritto di audit, risoluzione per violazione, obbligo di segnalazione e formazione.

8. Registrazioni e conservazione

Tutte le DD sono registrate nel DMS (cartelle Progetti, Fornitori, HR, Transazioni) con codifica e versione. Conservazione minima: 5 anni (o maggiore se richiesto da legge/contratti). Accessi profilati (Compliance, Direzione, OdV, process owner).

Registro	Campo chiave	Esempio	Owner	Frequenza aggiorn.	Formato	Ubicazione
Registro DD Progetti	ID commessa; risk score; esito; condizioni	C-2026-015; 12; OK con condizioni	Uff. Gare/Compliance	On event	Modulo + dossier	DMS/Progetti/DD
Registro DD Soci in affari	Partita IVA; risk rating; clausole; scadenza rinnovo	IT123…; Alto; clausole rinforzate; 12/2026	Acquisti	Mensile	Portale fornitori	DMS/Fornitori/DD
Registro DD Transazioni	Tipo; importo; approvazioni; IBAN verificato	Consulenza; €45k; doppia firma	Amministrazione	Mensile	Checklist + allegati	DMS/Finanza/DD
Registro DD HR	Ruolo; conflitti; formazione; esito	Buyer Sr.; no conflitti; attestato	HR	On event	Checklist HR	DMS/HR/DD

9. Riesame periodico e trigger di aggiornamento

Riesame: Basso = biennale; Medio = annuale; Alto = semestrale. Trigger on event: cambio proprietà/beneficial owner; nuove giurisdizioni; variazioni di valore >20%; segnalazioni WB; esiti audit negativi; sanzioni/PEP; comportamenti anomali (pagamenti fuori contratto).

10. Tutela dati e trasparenza

I dati personali trattati nelle DD sono gestiti secondo GDPR (minimizzazione, base giuridica, informative, tempi di conservazione). Per verifiche PEP/sanzioni si impiegano fonti legittime e proporzionate al rischio.

11. Allegati – Modelli operativi

A. Check-list DD Progetti (screening rischio, red flags, decisioni)

B. Check-list DD Fornitori/Partner (identità, proprietà effettiva, integrità, clausole)

C. Check-list DD Transazioni (coerenza contrattuale, IBAN, approvazioni)

D. Check-list DD HR (conflitti, referenze, formazione, deleghe)

12. Approvazione

Nome e ruolo	Firma	Data
Amministratore Unico / Compliance / RSGA	_____	02/01/2025

cosbotek