PROCEDURA CONTROLLI FINANZIARI E NON FINANZIARI – §8.3 e §8.4 ISO 37001

UNI ISO 37001:2016 – COSBOTEK S.r.l.

1. Scopo e campo di applicazione

La presente procedura definisce i controlli finanziari (§8.3) e non finanziari (§8.4) del Sistema di Gestione Anticorruzione (ABMS) di COSBOTEK, con riferimento a: autorizzazione e pagamento, tracciabilità dei flussi e dei giustificativi, red flags, controlli su approvvigionamenti/contratti/vendite, coerenza con deleghe e procure, campionamenti e verifiche.

2. Ruoli, segregazione dei compiti (SoD) e coerenza con deleghe/procure

Ruolo	Responsabilità principale	Poteri (deleghe/procure)	Limitazioni/SoD	Evidenze richieste
Richiedente/Process owner	Richiesta acquisto/spesa; allega giustificativi	Nessuna firma dispositiva	Non approva; non paga	Richiesta/PO; giustificativi
Approvatore di spesa	Autorizza la spesa entro limiti di delega	Delega economica per centro di costo/soglia	Non crea/contabilizza pagamenti	Firma digitale su richiesta/PO
Acquisti	Emissione PO; qualifica fornitori; contratti	Entro policy; nessun potere di pagamento	Non approva pagamento	PO; contratto; vendor master log
Amministrazione	Contabilizza; riconcilia; prepara pagamenti	Firma contabile	Non approva la spesa; non emette PO	Registrazioni; 3-way match
Direzione	Approvazioni straordinarie; pagamenti oltre soglia; procure	Procura/firma legale secondo delibera	Doppia firma > soglia	Delibere; firma digitale
Compliance/RSGA	Controlli ABMS; campionamenti; red flags	Nessun potere di pagamento	Indipendenza dalle operazioni	Report controlli; check-list

Le deleghe/procure sono pubblicate nel DMS con codifica e scadenza; ogni approvazione/pagamento è coerente con i limiti previsti. Le anomalie (superamento soglie, conflitti SoD) attivano escalation a Direzione e Compliance.

3. Flusso di autorizzazione e pagamento (§8.3 – controlli finanziari)

Fase	Attività/controllo	Responsabile	Soglie/criteri	Output/Evidenza	Red flags (estratto)
Richiesta spesa	Descrizione, causale, centro costo, allegati	Process owner	Completezza dati	Richiesta firmata	Urgenze immotivate; causali generiche
Autorizzazione	Conferma budget e necessità; limiti delega	Approvatore	Entro soglia delega	Autorizzazione digitale	Approvatore coinvolto nel pagamento
Ordine/Contratto	PO/contratto con clausole etiche; tracciabilità	Acquisti	Fornitore qualificato	PO; contratto	Fornitore nuovo non qualificato
Ricezione/Verifica	3-way match (PO–DDT–Fattura) + IBAN verificato	Amministrazione	> € X: conferma ricezione indipendente	Check-list 3WM; esito Co.Ge.	Fatture senza PO; IBAN cambiato
Pagamento	Doppia firma; segregazione proposta/esecuzione	Amministrazione + Direzione	> soglia Y: firma Direzione	Distinta bonifici firmata	Pagamenti a terzi non contrattuali
Riconciliazione	Riconciliazioni bancarie; analisi scostamenti	Amministrazione	Mensile	Report riconciliazioni	Scritture manuali atipiche

4. Tracciabilità dei flussi e dei giustificativi

Tutti i passaggi sono tracciati in DMS/ERP: richiesta → autorizzazione → PO/contratto → 3-way match → distinta pagamento → estratto conto. I giustificativi (contratti, DDT, fatture, note spese con scontrini/fatture, report eventi per sponsorizzazioni) sono archiviati con riferimento univoco alla commessa/centro di costo; i cambi IBAN richiedono verifica indipendente e doppia autorizzazione.

5. Elenco red flags considerati (orientativo)

- Fatture senza riferimento a PO/contratto o con descrizioni vaghe;
- Modifica IBAN/beneficiario non comunicata su canale ufficiale;
- Intermediari/consulenti non giustificati con success fee sproporzionate;
- Pagamenti urgenti/non programmati a ridosso di decisioni di gara/varianti;
- Omaggi/spese oltre soglia o non documentate;
- Richieste di pagamento a soggetti terzi o in giurisdizioni non collegate alla fornitura;
- Fornitori con proprietà poco trasparente o legami con PA;
- Sconti anomali, note di credito ricorrenti senza giustificazione;
- Divisione artificiosa di ordini per eludere soglie di autorizzazione;
- Conflitti di interesse dichiarati/emersi su ruoli coinvolti.

cosbotek

6. Controlli non finanziari (§8.4): approvvigionamenti, contratti, vendite

Area	Controllo/standard	Frequenza/livello rischio	Responsabile	Evidenze	Note/collegamenti
Approvvigionamenti	Vendor master a 4 occhi; qualifica e clausole etiche; check conflitti	Onboarding; rinnovo annuale (alto rischio semestrale)	Acquisti + Compliance	Registro fornitori; DD; clausole	Allineato §8.2 DD
Contratti	Clausole anticorruzione obbligatorie; diritto audit; no intermediari non autorizzati	Sempre; revisione legale su alto rischio	Acquisti/Legale/Compliance	Contratto firmato; check-list clausole	Coerenza deleghe/procure
Vendite	Sconti e condizioni speciali approvati entro delega; verifica partner; tracciabilità varianti	Per offerta; trimestrale a campione	Commerciale + Direzione	Report offerte; approvazioni	Raccordo con Modello 231 Appalti
Cantieri	Checklist interazioni PA; registro visitatori; rotazione incarichi sensibili	Trimestrale; on event	RSGA + D. Tecnica	Verbali cantiere; registro	Collegato piano monitoraggio
Note spese/omaggi	Limiti valori; pre- autorizzazione; documenti originali	Mensile	Amministrazione + Compliance	Registro spese; ricevute	Policy omaggi/spese

7. Piano di campionamento e verifiche

Ambito	Campione/criteri	Frequenza	Esecutore	Griglia di verifica	Evidenze/Output
Pagamenti	≥ 20% mensile, risk-based (importo, nuovo IBAN, Paese)	Mensile	Amministrazione + Compliance	Doppia firma; coerenza contratto; IBAN	Report controlli; lista eccezioni
PO/Contratti	Campione 10%/trim. (alto rischio 25%)	Trimestrale	Acquisti + Compliance	Clausole etiche; firma delegata; DD fornitore	Check-list firmata; azioni
Vendite/offerte	Campione 10% offerte e varianti	Trimestrale	Commerciale + Compliance	Approvi entro delega; tracciabilità	Report scostamenti
Spese/omaggi	100% > soglia; 20% sotto soglia	Mensile	Amministrazione	Giustificativi; pre- autorizz.	Registro controlli; rimborsi bloccati

8. Escalation, blocchi e rimedi

In presenza di red flags o scostamenti, il pagamento/ordine è sospeso. La Compliance apre un ticket di indagine; la Direzione delibera lo sblocco o la risoluzione del contratto. Sono avviate azioni correttive/preventive e, se del caso, segnalazioni a OdV/RPCT.

9. Registrazioni e conservazione

Registro	Contenuto minimo	Owner	Conservazione	Ubicazione	Accessi
Registro autorizzazioni	Richiesta, approvatore, soglia, data	Amministrazione	≥ 5 anni	DMS/ERP	Profilati
Registro pagamenti	Beneficiario, IBAN, causale, firme	Amministrazione	≥ 5 anni	DMS/ERP	Profilati
Registro controlli/campionamenti	Ambito, campione, esiti, azioni	Compliance	≥ 5 anni	DMS/ABMS	Compliance/Direzione/OdV
Registro red flags	Caso, natura, azioni intraprese	Compliance	≥ 5 anni	DMS/ABMS	Riservato

10. Approvazione

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