ERP LUCCA S.r.l. documento di analisi dei rischi ex D.lgs. n. 231/01

SECONDO LE LINEE GUIDA CONFINDUSTRIA E GLI STANDARD UNI EN ISO 31000:2010

COPIA CONTROLLATA ☑ N. [ ] COPIA NON CONTROLLATA ❑

Revisioni e approvazioni

Rev. n.	**Data Approvazione (CDA)**
Prima adozione	
1	
2	
3	
4	

PROPRIETÀ E DIFFUSIONE

DOCUMENTO DI ANALISI DEI RISCHI

1.SCOPO E CAMPO DI APPLICAZIONE

Il presente documento fornisce evidenza, in formato descrittivo, delle modalità e dei risultati finali con cui è stata operata la valutazione del rischio di commissione delle fattispecie di reato previste dal D.lgs. 231/01 nello svolgimento dei processi di gestione aziendali da parte dei soggetti responsabili delle singole attività in cui tali processi si articolano.

In funzione della valutazione dei rischi, **ERP LUCCA S.r.l.** (di seguito anche: Impresa) individua i necessari protocolli di controllo (sotto forma di regolamenti, politiche, procedure, istruzioni operative, etc.) atti a ridurre il livello di rischio rilevato entro livelli di rischi (rischio residuo) considerati accettabili.

2.RIFERIMENTI NORMATIVI

Si riportano i riferimenti normativi a cui il presente documento si richiama:

- D.lgs. 8 giugno 2001 n. 231 " Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica a norma dell'art. 11 della legge 29 settembre 2000 n. 300".
- Linee Guida di Confindustria per la costruzione dei modelli di organizzazione, gestione e controllo ex D.lgs n. 231/01;
- Standard UNI EN ISO 31000: 2010 "gestione del rischio - principi e linee guida";
- Legge n. 190/12, P.N.A. e Delibera Anac. n. 1134/17;

3.TERMINI E DEFINIZIONI

Si riporta la definizione degli acronimi utilizzati nel presente documento:

- MOG: acronimo di Modello di Organizzazione e Gestione ai sensi del D.lgs. n. 231/01 (Nota: inteso sia come sistema di gestione sia come documento che descrive tale sistema di gestione);
- ODV: acronimo di Organismo di Vigilanza ai sensi del D.lgs. n. 231/01;
- Rischio: effetto dell'incertezza sugli obiettivi (ISO 31000, p.to 2.1);

- Gestione del Rischio (Risk Management): attività coordinate per dirigere e controllare un'organizzazione relativamente al rischio (ISO 31000, p.to 2.2);
- Piano di Gestione del Rischio: schema che specifica l'approccio, i componenti della gestione e le risorse che devono essere applicate alla gestione del rischio (ISO 31000, p.to 2.8);
- Processo di gestione del rischio: applicazione sistematica di politiche, procedure e prassi alle attività di comunicazione, consultazione, definizione del contesto, identificazione, analisi, stima, trattamento, monitoraggio e riesame del rischio (ISO 31000, p.to 2.10);
- Stabilire il contesto: definire i parametri interni ed esterni che devono essere presi in considerazione nella gestione del rischio e stabilire lo scopo e i criteri del rischio per la politica di gestione del rischio (ISO 31000, p.to 2.11);
- Valutazione del rischio: processo globale d'identificazione del rischio, analisi del rischio e stima del rischio (ISO 31000, p.to 2.16);
- Identificazione del rischio: processo di ricerca, riconoscimento e descrizione dei rischi (ISO 31000, p.to 2.17);
- Fonte del rischio: elemento che solo o in combinazione ha l'intrinseco potenziale di far sorgere il rischio (ISO 31000, p.to 2.18);
- Evento: occorrenza o cambiamento di un particolare insieme di circostanze (ISO 31000, p.to 2.19);
- Profilo del rischio: descrizione di un insieme di rischi (ISO 31000, p.to 2.22);
- Analisi del rischio: processo per comprendere la natura del rischio e per determinare il livello del rischio (ISO 31000, p.to 2.25);
- Conseguenze: risultato di un evento sugli obiettivi (ISO 31000, p.to 2.20);
- Probabilità: possibilità che accada qualcosa (ISO 31000, p.to 2.21);
- Livello del Rischio: magnitudine di un rischio espresso nei termini della combinazione delle conseguenze e della loro probabilità (ISO 31000, p.to 2.25);
- Stima del rischio: processo di comparazione dei risultati dell'analisi del rischio con criteri del rischio al fine di determinare se il rischio e la sua magnitudo è accettabile o tollerabile (ISO 31000, p.to 2.26);
- Criterio del Rischio: termini di riferimento a fronte dei quali la significatività di un rischio è valutata (ISO 31000, p.to 2.24);

- Trattamento del rischio: processo per modificare il rischio (ISO 31000, p.to 2.27);
- Controllo: misura che modifica il rischio (ISO 31000, p.to 2.28);
- Rischio residuo: rischio che rimane dopo il trattamento del rischio (ISO 31000, p.to 2.29);
- Piano della prevenzione della corruzione: documento elaborato dall'RPCT e adottato dall'organo gestorio in attuazione della Legge n. 190/12.

4. METODOLOGIA DI ANALISI DEL RISCHIO

Per Analisi dei Rischi si intende lo studio delle minacce e delle vulnerabilità a cui sono soggetti i processi individuati.

Per l'analisi dei rischi è stato applicato il cosiddetto "*Risk Approach*"[1] ovvero una metodologia volta alla determinazione del rischio associato a precisati pericoli o sorgenti di rischio. Essa parte da una verifica dello stato dell'arte "*As is analysis*", si sviluppa nella ricerca e successiva valutazione (*to assess*) del rischio "*Risk Assessment*" e si conclude con la gestione (*to manage*) del rischio "*Risk Management*".

Analizzare i rischi significa quindi, tramite il ***Risk Assessment***, identificare, analizzare e valutare il rischio presente nell'ambito/processo aziendale considerato, stimandone il valore e verificandone il livello di accettabilità per poi ordinare i vari rischi secondo priorità, onde poter orientare il ***Risk Management*** facilitando l'individuazione di soluzioni per la mitigazione dei rischi stessi (*Risk Mitigation)*.

Secondo la metodologia sopra descritta, il rischio di commissione di un Reato è stato valutato preliminarmente ipotizzando una situazione di assoluta "assenza di controlli" sul processo (ovvero, il rischio lordo o potenziale). Sono state poi individuate, per ciascun processo-reato, le attività di controllo esistenti.

[1] Confindustria (2014) parla di Risk approach (pag. 28) mentre la circolare GdF 83607/2012 Vol. III parla espressamente delle sue componenti "Risk Assessment" "Risk Management" (pag. 76)

Solo una volta individuata e verificata l'efficacia delle attività di controllo, è stato pertanto definito il "rischio netto" di commissione di ciascun Reato, il rischio cioè che le "fattispecie di reato possono essere attuate rispetto al contesto operativo interno ed esterno in cui opera l'azienda" (Confindustria, Linee Guida).

Il perché della necessità di identificare e valutare separatamente il "rischio lordo" (cioè, si ribadisce, il rischio potenziale, di commissione di un Reato in un'ipotetica situazione di assenza di controlli) dal "rischio netto" (ovvero, il rischio residuale, di commissione del reato nel reale contesto operativo in cui opera l'azienda, sulla base della vulnerabilità del sistema di controllo interno) è evidente: ragionando sul solo "rischio netto" si sarebbe sottostimata la rischiosità del processo e trascurata l'importanza del corretto funzionamento del sistema di controllo.

La distinta valutazione del rischio lordo, del sistema dei controlli (vulnerabilità) e del conseguente indice di intervento, per ciascun processo-Reato, risulta indispensabile per pianificare secondo priorità gli interventi necessari per colmare gli eventuali *gap* del sistema di controllo (*gap analisys*) e poi determinare il rischio residuo.

Tali interventi sono pianificati quindi quando l'indice di intervento evidenzia un livello rischio netto non sostenibile e pertanto non può essere accettato da chi ne è esposto. A questo scopo nel panorama del rischio è stato tracciato un limite di tolleranza del rischio (c.d. rischio accettabile) al di sopra del quale devono essere prese adeguate misure che assicurino la sua mitigazione (*risk mitigation*).

Un concetto assolutamente nodale nella costruzione di un sistema di controllo preventivo è quello di rischio accettabile.

Nella progettazione del sistema di controllo a tutela dei rischi di *business*, nei termini sopra indicati, il rischio è ritenuto accettabile in quanto i controlli aggiuntivi rischiano di "costare" più della risorsa da proteggere e ciò assume maggiore importanza per le piccole-medie imprese come ERP LUCCA S.r.l..
Nel caso del D.lgs. n. 231/01 la logica economica dei costi, applicata nel caso di specie, non può però essere un riferimento utilizzabile in via esclusiva. Ai fini dell'applicazione delle norme del Decreto è stata definita una soglia effettiva che consente di porre un limite alla quantità/qualità delle misure di prevenzione da

introdurre per evitare la commissione dei reati considerati. In assenza di una previa determinazione del rischio accettabile, la quantità/qualità di controlli preventivi istituibili è infatti virtualmente infinita, con le intuibili conseguenze in termini di operatività aziendale.

Come è stato evidenziato nelle Linee Guida, peraltro, la soglia concettuale di accettabilità del rischio nei reati dolosi è rappresentata da un sistema di prevenzione tale da non poter essere aggirato se non FRAUDOLENTEMENTE.

Diversamente, la soglia concettuale di accettabilità, agli effetti esimenti del decreto 231, va diversamente modulata in relazione ai reati di natura colposa, in quanto l'elusione fraudolenta dei modelli organizzativi appare incompatibile con l'elemento soggettivo dei reati colposi, in cui manca la volontà dell'evento lesivo. In questa ipotesi, la soglia di rischio accettabile è rappresentata dalla realizzazione di una condotta in violazione degli obblighi giuridici che regolano la singola fattispecie, in mancanza delle condizioni previste dall'art. 6, comma primo lett. a), b) e d) e quindi quando non viene adottato ed efficacemente attuato il modello organizzativo, non è stato istituito l'apposito Organismo di vigilanza ed è stata omessa o insufficiente la vigilanza da parte dell'Organismo stesso.

Pertanto, il sistema di controllo preventivo come sopra articolato, deve risultare in grado di:

- escludere che un qualunque soggetto operante all'interno dell'Impresa possa giustificare la propria condotta adducendo l'ignoranza delle direttive aziendali;
- evitare che, nella normalità dei casi, il reato possa essere causato dall'errore umano (dovuto anche a negligenza o imperizia) nella valutazione delle direttive aziendali.

Si può in definitiva affermare che i rischi che si sono posizionati sopra questo limite in linea di principio non sono stati tollerati ed hanno determinato un "indice di intervento" elevato, mentre i rischi sotto questo limite sono stati ritenuti accettabili e per questi l'"indice di intervento" si è posizionato su un livello basso, risultando sufficienti le norme di comportamento e le prescrizioni (generali e specifiche) contenute nelle diverse parti del "Modello" e i presidi già in uso in azienda.

5. APPROCCIO OPERATIVO

L'Impresa ha provveduto, tramite un Gruppo di Lavoro composto da professionisti specializzati in materia di controllo interno, in campo legale, sicurezza sul lavoro e ambientale, applicando la metodologia sopra descritta, all'analisi dei rischi, assumendo a riferimento lo standard UNI EN ISO 31000:2010 "gestione del rischio – principi e linee guida", adattandolo con la finalità di elaborare un modello organizzativo coerente con la specifica attività della Società, conformemente a quanto previsto dal D.lgs. n. 231/2001.

Detta attività si è basata su interviste svolte nel corso del 2020 e confermate nel mese di gennaio del 2022 in concomitanza con l'aggiornamento annuale del PTCPT. I Soggetti intervistati sono i seguenti: Il Dirigente, il RPCT, il Referente del Sistema di Gestione della qualità.. È stata inoltre esaminata la documentazione societaria e aziendale acquisita (statuto, regolamenti e procedure, visura camerale ecc.).

Il processo di analisi dei rischi è stato integrato da una revisione operata da un consulente esterno appositamente incaricato ed avente ad oggetto la verifica degli impatti delle modifiche intervenute sul D.lgs. n. 231/01 nel corso del 2023, del 2024 e del 2025 fino alla data di approvazione dell'aggiornamento del Modello 231, di cui il presente documento fa parte, da parte del CdA. L'analisi si è sviluppata secondo la metodologia sopra descritta, è stato articolato nelle fasi di seguito sintetizzate e poi analiticamente illustrate.

- ✓ **Individuazione del contesto**: Il contesto di riferimento in cui opera l'Impresa determina la tipologia dei rischi da prendere concretamente in considerazione. Mediante la considerazione del contesto di riferimento, l'Impresa effettua una prima valutazione "sintetica" del proprio profilo di rischio. Questo al fine di rendere più concreta ed operativa la valutazione dei rischi condotta in modo analitico con riferimento a specifici pericoli.

  Mediante tale approccio, che riprende la logica dell'analisi "costi / benefici", l'Impresa focalizza la propria attenzione solo sulle fattispecie di rischio che, per quanto improbabili, presentano comunque una ragionevole verosimiglianza. In questa fase sono quindi valutati come non pertinenti (ed esclusi da ulteriore valutazione) tutte quelle fattispecie di pericoli che presentano un grado di verosimiglianza di fatto pari a zero. Il contesto è costituito dal più generale "ambiente" in cui l'Impresa opera, caratterizzato dai seguenti elementi:
  - Contesto settoriale e missione strategica;
  - Contesto territoriale;
  - Contesto organizzativo;
  - Contesto economico, finanziario, patrimoniale;
- ✓ **Risk – Assessment :** si occupa dell'identificazione dei reati presupposto applicabili e dei processi a rischio, della determinazione della loro probabilità di accadimento e del loro impatto (valutazione dei rischi potenziali), per poi individuare, ad esito dell'*as is analisys* ovvero della valutazione del sistema di controllo interno (SCI), le priorità di intervento. La valutazione del livello di rischio (*Risk Assessment*) di commissione, nell'ambito dei processi aziendali, di uno dei reati previsti dal D.lgs. n. 231/01 (c.d. "rischio-reato") è una fase essenziale del processo di costruzione di un modello di organizzazione, gestione e controllo conforme ai requisiti del D.lgs. n. 231/01.
- ✓ **Risk – Mitigation:** rientra nell'alveo delle attività di *Risk Management***;** serve a determinare ed implementare, sulla base della *gap-analisys,* le azioni correttive necessarie alla riduzione del rischio e comunque al mantenimento di quest'ultimo nelle soglie di accettabilità.
- ✓ **Evaluation – valutazione del rischio "231" (rischio residuale o residuo):** individuazione del rischio netto quale risultato della strategia di *risk-response* attuata.

- ✓ **Disegno del Modello e piano di azione per la sua efficace attuazione:** si tratta pianificare le attività necessarie per assicurare la funzione "esimente" del Modello.

Di seguito sono schematizzate le fasi sopra elencate, previa individuazione del "contesto":

Per quanto concerne specificatamente i reati in materia di salute e sicurezza sul lavoro, sono stati individuati come a rischio i processi contemplati dall'art. 30 del D.lgs. n. 81/08 così come previsto dalle citate Linee Guida emanate da Confindustria.

I risultati di tale attività sono contenuti all'interno della parte speciale del "Modello 231" dedicata ai reati in materia di SSLL.

Il processo di analisi dei rischi di ERP LUCCA S.r.l., secondo la metodologia sopra descritta, è stato sviluppato come di seguito illustrato.

6. IL CONTESTO IN CUI OPERA ERP LUCCA S.r.l..

L'analisi del contesto (esterno ed interno) costituisce la prima fase del processo di gestione del rischio quale strumento attraverso cui ottenere le informazioni

necessarie a comprendere il livello dei rischi sulla base delle specificità dell'ambiente in cui opera o per via delle caratteristiche organizzative interne.

6.1. contesto esterno

Per quanto riguarda il contesto esterno sono stati approfonditi gli aspetti relativi alla situazione socio-economica in cui la società si trova ad operare.

È emerso che la società non opera in regime di concorrenza per le ragioni illustrate nel paragrafo sulla *mission*, pertanto tutte le attività sono svolte con sostanziale esclusiva.

Tale quadro è stato composto recependo la disamina contenuta nel Piano della prevenzione della corruzione 2023-2025 adottato come stabilito dalla Legge n. 190/12.

6.2. contesto interno

6.2.1 gli assetti proprietari

Edilizia Residenziale Pubblica per la Provincia di Lucca, (di seguito ERP Lucca S.r.l.) è la Società costituita tra i comuni del LODE Lucchese.

6.2.2. missione strategica

La Società è stata costituita per la gestione unitaria, il recupero e la nuova realizzazione, del patrimonio d'edilizia residenziale pubblica in conformità a quanto disposto dalla Legge Regionale 77/1998. La legge di riforma citata, mentre conferisce alla Regione i compiti di programmazione e d'indirizzo, assegna ai Comuni la proprietà del patrimonio residenziale pubblico e le competenze per una più equa e organica politica sociale della casa. I Comuni associati della provincia di Lucca hanno poi conferito ad ERP Lucca S.r.l., tramite un apposito contratto di servizio (rinnovato fino al 31.12.2027, cinque anni con atto ai rogiti del Notaio Domenico Costantino, registrata a Lucca il 21 novembre 2022 al n. 8719 Serie 1T), i relativi compiti che sono assai rilevanti, sia per l'importanza sociale del soddisfacimento del diritto alla casa, sia per la considerevole dimensione del

patrimonio d'edilizia residenziale pubblica che l'azienda gestisce per conto dei Comuni.

6.2.3 contesto organizzativo

A) *Governance* e struttura organizzativa

Il Sistema di amministrazione e controllo della società è rappresentato dal Sistema Tradizionale.

Assemblea dei Soci

Organo Amministrativo

La società è amministrata da un CdA.

Gli amministratori sono nominati dall'Assemblea.

Tale organo è investito di tutti i poteri di ordinaria e straordinaria amministrazione occorrenti per il raggiungimento dell'oggetto sociale, ferme restando le decisioni riservate dalla legge o dallo statuto alla competenza dei soci.

Deleghe e procure

La Società ha attuato uno specifico sistema di autorizzazione alla spesa e un sistema di poteri di firma, alla luce del quale è previsto che solo i soggetti muniti di formali e specifici poteri possano assumere impegni verso terzi in nome o per conto della Società stessa.

Il sistema organizzativo della Società è improntato a principi generali di:

a) chiara descrizione delle linee di riporto;

b) conoscibilità, trasparenza e pubblicità dei poteri attribuiti (all'interno della Società e nei confronti dei terzi interessati);

c) chiara e formale delimitazione dei ruoli, con una completa descrizione dei compiti di ciascuna funzione, dei relativi poteri e responsabilità.

La rappresentanza della società di fronte ai terzi ed in giudizio e la firma sociale spettano al Presidente e al Dirigente per le materie ad essi attribuite all'atto della nomina.

In generale, il sistema di deleghe e procure è caratterizzato da elementi di certezza ai fini della prevenzione dei reati previsti dal D.Lgs. n. 231/2001, consentendo la gestione efficiente dell'attività aziendale.

Tale sistema viene delineato nel protocollo appartenente al Modello, denominato "Protocollo per la formazione della volontà della Società" in corso di aggiornamento in relazione alla nuova governance aziendale e all'organigramma conseguente.

Direzione, coordinamento e controllo analogo.

La società opera con la modalità dell'*in house providing* e pertanto è assoggettata al controllo analogo congiunto da parte dei Comuni soci .

I Comuni soci, in attuazione del controllo analogo, assumono particolari poteri di indirizzo e di gestione declinati nello Statuto e dei contratti di servizio anche in deroga alle previsioni del Codice civile (D.lgs. n. 175/16).

La società ha elaborato un organigramma funzionale con evidenza delle responsabilità e un organigramma in materia di SSLL.

B) Controllo

La vigilanza sulla legalità e la revisione legale dei conti sono state affidate ad un Collegio Sindacale di tre membri, ad un RPCT e ad un OdV, nominato ai sensi del D.lgs. n. 231/01, che operano in stretto coordinamento tra loro anche. All'OdV spettano altresì le funzioni analoghe a quelle degli OiV ai fini dell'attestazione sull'assolvimento degli obblighi di trasparenza dettati dal D.lgs. n. 33/13 in attuazione della Legge n 190/12.

C) Struttura amministrativo contabile

La struttura contabile – amministrativa è interna.

La struttura interna si occupa anche del processo di redazione del bilancio di esercizio, in collaborazione con uno studio professionale esterno che assiste inoltre la società nelle fasi di elaborazione/invio dei dichiarativi fiscali.

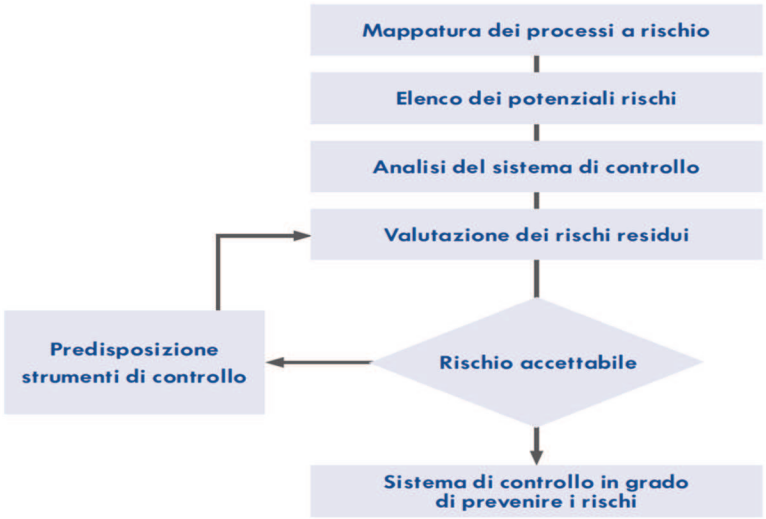
7. RISK ASSESSMENT

Le fasi seguite per giungere alla formulazione di un quadro di sintesi dell'esposizione al rischio "231" dell'intera Organizzazione, sono di seguito elencate e successivamente approfondite:

1) Ricognizione delle fattispecie di reato presupposto applicabili.
2) Mappatura dei processi a rischio di commissione di reati presupposto (mappatura dei rischi per processo).
3) Valutazione dell'esposizione al rischio potenziale per processo.
4) Esame dell'efficacia dei presidi di controllo posti a contenimento dei rischi potenziali *(As is analisys)*.
5) determinazione dell'indice di intervento.

All'esito dell'attività di *risk assessment*, si è provveduto:

- alla gap analysis con l'identificazione dei punti di miglioramento, con la formulazione di appositi suggerimenti (c.d. Risk Mitigation) e all'elaborazione del "piano di azione" (cap. 8).
- Alla determinazione del rischio netto (cap. 9)



1) Ricognizione delle fattispecie di reato presupposto applicabili.

Avuto riguardo alla tipologia dei reati richiamati nel D.lgs. n. 231/01, si è provveduto ad effettuare un'analisi anche storica dell'azienda, dei suoi processi operativi interni e delle attività che la stessa generalmente compie per la realizzazione del proprio scopo sociale, al fine di identificare e valutare l'esistenza di situazioni a rischio di commissione dei reati sopra citati.

La probabilità di commissione di reati rilevanti ai fini del D.lgs. n. 231/01, è stata individuata in funzione del contesto descritto nei paragrafi precedenti, della storicità e della ritmicità/frequenza dei processi che hanno permesso di definire in generale come "non materiale" il rischio correlato a determinate tipologie di reato.

L'analisi delle aree potenzialmente a rischio non ha riguardato alcune tipologie d reati per i quali, pur non potendosi escludere del tutto la loro astratta verificabilità, la loro realizzazione in concreto appare poco probabile in relazione all'attività svolta dalla società ed in particolare considerando che il presupposto affinché possa ricorrere la responsabilità amministrativa è rappresentato dal fatto che il reato sia compiuto nel suo interesse o a suo vantaggio.

Alla luce di tale verifica si ritiene che delle categorie di reati previsti fino ad oggi nel Decreto citato, risulti non significativa o sostanzialmente remota la probabilità astratta che possano essere commessi quelli ricompresi nelle categorie che seguono, le quali non sono state considerate nella valutazione dei rischi.

Art. 25-sexiesdecies	Contrabbando (diritti di confine)
Art. 25-septiesdecies	Delitti contro il patrimonio culturale
Art. 25-duodevicies	Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali
L.n.146/2006	Reati transnazionali
Art. 25-quaterdecies	Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati
Art. 25-terdecies	Reati di razzismo e xenofobia
Art. 25-duodecies	Disposizioni contro le immigrazioni clandestine
Art. 25-novies	Delitti in materia di violazione del diritto d'autore
Art. 25-octies.1	Delitti in materia di strumenti di pagamento diversi dai contanti
Art. 25-sexies	Reati finanziari o abusi di mercato
Art. 25-quinquies	Delitti contro la personalità individuale

Art. 25-quater.1	Pratiche di mutilazione degli organi genitali femminili
Art. 25-quater	Reati con finalità di terrorismo o di eversione dell'ordine democratico
Art. 25-bis.1	Delitti contro l'industria ed il commercio
Art. 25-bis	Falsità in monete
Art. 24-ter	Reati di criminalità organizzata
Art. 25-undevicies	Delitti contro gli animali"): le fattispecie (uccisione, maltrattamento, combattimenti, spettacoli vietati, ecc.) diventano reati-presupposto ai fini della responsabilità amministrativa degli enti (decorrenza 1/7/2025).

Per quanto attiene ai reati contro e nei rapporti con la P.A., ivi compresa la fattispecie della "corruzione tra privati" e relativa istigazione, contemplati nella Legge 190/12, si precisa che sono già stati valutati in termini di rischio e trattati nell'ambito del Piano della prevenzione della corruzione, aggiornato annualmente a norma della Delibera Anac n. 1134/17 e del P.N.A. il quale per espressa previsione normativa rappresenta parte integrante e sostanziale del Modello 231. La Parte Speciale del Modello 231 ad essi dedicata è limitata ai profili rilevanti ai fini dell'applicazione del D.lgs. n. 231/01.

2) mappatura dei processi a rischio di commissione di reati presupposto

Per ciascuna delle categorie di "reati 231" valutate preliminarmente con un livello di probabilità di accadimento non remota rispetto al contesto in cui la società opera, sono state pertanto effettuate le valutazioni di rischio più approfondite, focalizzando l'attenzione sui cosiddetti processi sensibili, ossia i processi nell'ambito dei quali sia più verosimile la commissione dei reati 231 e la loro tipologia.

La struttura organizzativa, tenuto conto del contesto in cui la società opera, in precedenza descritto, è stata pertanto sottoposta ad un preliminare mappatura dei processi a rischio.

All'esito di tale lavoro, è stato definito l'elenco dei processi potenzialmente "a rischio reato 231", per i quali è stato ritenuto astrattamente sussistente il rischio di commissione dei reati, tra quelli indicati dal Decreto, riconducibili alla tipologia di attività svolta dalla Società.

È stata nel contempo incentrata l'attenzione sui cosiddetti "processi strumentali", ossia i processi nel cui ambito ed in linea di principio potrebbero crearsi "strumenti" ovvero configurarsi "condizioni o mezzi" per la commissione dei reati di cui al D. Lgs.

231/01 ed in grado di creare le condizioni all'interno dei processi sensibili, per l'effettiva commissione dei reati.

Tra questi, sono stati presi in considerazione tutti quei processi afferenti la provvista e la gestione di risorse finanziarie ed in particolare quelli che possono essere utilizzati per la creazione di fondi liberamente disponibili (ciclo attivo e passivo, gestione risorse finanziarie ecc.).

Nell'allegato 1 è stata fornita evidenza dei processi a rischio potenziale di commissione reato mappati, con relativa associazione alle tipologie di reato rilevanti, alle aree aziendali e alle attività sensibili.

Di seguito la tabella mostra il dettaglio delle categorie di reato prese in esame ai fini della valutazione dei "rischi 231".

Reato (categoria)	ARTICOLO
24	Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture [Articolo modificato dalla L. 161/2017 e dal D.Lgs.n.75 del 14 luglio 2020]
24bis	Delitti informatici e trattamento illecito di dati [Articolo aggiunto dalla L. n. 48/2008, modificato dai D.Lgs. n.7 e n. 8/2016, dal D.L. n. 105/2019 e da Legge n.90 del 28 Giugno 2024]
25	Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilita', corruzione [Articolo modificato dalla L. n. 190/2012, dalla Legge n. 3 del 9 gennaio 2019 dal D.Lgs.n.75 del 14 luglio 2020 e dalla Legge n.112 dell'8 agosto 2024]
25ter	Reati societari [Articolo aggiunto dal D.Lgs.n.61/2002, modificato dalla L. n. 190/2012, dalla L. 69/2015 e successivamente dal D.Lgs. n.38/2017 e da D.Lgs.n.19 del 2 Marzo 2023]
25undecies	Reati ambientali [Articolo aggiunto dal D.Lgs.n.121/2011, modificato dalla L. n. 68/2015 e da D.Lgs. n. 21/2018]
25octies	Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza

	illecita, nonché autoriciclaggio [Articolo aggiunto dal D.Lgs.n.231/2007; modificato dalla L. n. 186/2014 e da D.Lgs.n.195 dell'8 novembre 2021]
25octies 1	Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori [Articolo aggiunto dal D.Lgs.n.184 del 18 novembre 2021e modificato da D.L.10 agosto 2023 n.105 coordinato con la Legge di conversione n.137 del 9 ottobre 2023]
25quinquiesdecies	Reati tributari [Articolo aggiunto dal D.L. n.124/2019 coordinato con Legge di conversione n.157/2019 e modificato dal D.Lgs.n.75/2020. Indebita compensazione (Art. 10-quater D.Lgs.n.74 inserito da D.Lgs.n.75 del 14 luglio 2020 e modificato da D.Lgs n. 87 del 14 Giugno 2024)
25decies	Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria [Articolo aggiunto dalla L. n. 116/2009]
25septies	Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro [Articolo aggiunto dalla L. n. 123/2007]

La prossima tabella mette in relazione i reati astrattamente rilevanti con le responsabilità (funzioni aziendali).

MATRICE REATI - FUNZIONI

	Lucchesi Silvia - Manu.ne Ordinaria, Straordinaria e All. di Risulta	Gianluca Cassettai - Ragioneria	Lucchesi Silvia - Manu.ne Ordinaria, Straordinaria e All. di Risulta	Cardone Lorenza - Ufficio Personale	Lucchesi Silvia - Manu.ne Ordinaria, Straordinaria e All. di Risulta	Carli Roberta - Gare e appalti	Dinelli Laura - Servizi generali	Dinelli Anna Rita - S.I.A.	Gonnella Barbara - Patrimoniale	Gonnella Barbara - Segr. L.O.D.E. Lucchese – C.d.A.	Lucchesi Silvia - Manu.ne Straordinaria All. di Risulta	Maresca Paola - Morosità	Gonnella Barbara - Autogestioni e Condomini	Gonnella Barbara - Autogestioni e Condomini	TUTTE LE U.O.
24 (Reati commessi conntro la Pubblica Amministrazione)						✓					✓				
24bis (Delitti informatici e trattamento illecito di dati)								✓							
24ter (Delitti di criminalità organizzata)															
25 (Reati commessi nei rapporti con la Pubblica Amministrazione)	✓	✓		✓		✓	✓	✓	✓		✓	✓	✓	✓	
25decies (Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci						✓									
25duodecies(Impiego di lavoratori irregolari)															
25novies (Delitti in materia di violazione del diritto d'autore)															
25octies (Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, autoriciclaggio e ricettazione)	✓	✓				✓		✓	✓						
25quater (Reati con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali)															
25quinquies (Delitti contro la personalità individuale)															
25quinquiesdecies (Reati tributari)	✓	✓						✓	✓		✓				✓
25sepies (Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro)			✓	✓											
25sexies (Reati di abuso di mercato)															
25ter (Reati societari)		✓						✓	✓	✓	✓				
25undecies (Reati ambientali)					✓										

La tabella seguente mostra infine la correlazione reato-processo sensibile.

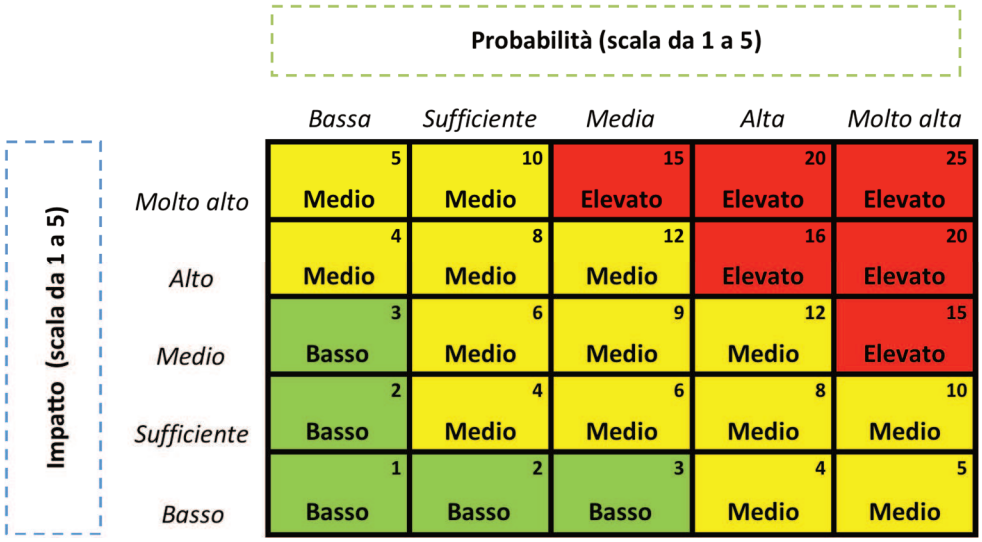
	Art. 24 (Reati commessi contro la Pubblica Amministrazione)	Art. 24bis Delitti informatici e trattamento illecito di dati	Art. 25 (Reati commessi nei rapporti con la Pubblica Amministrazione)	Art. 25 decies Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorita' giudiziaria	Art. 25 novies Delitti in materia di violazione del diritto d'autore	Art. 25 decies Reato di induzione a non rendere dichiarazione o a rendere dichiarazioni mendaci all'autorità giudiziaria	Art. 25 octies (Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita)	Art. 25 septies (Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro)	Art. 25 ter (Reati societari)	Art. 25 undecies (Reati ambientali)	Art. 25 quinquiesdecies (Reati tributari)
PRROCESSO											
Livello MEDIO di rischio LORDO per la categoria di reato	MEDIO	MEDIO	MEDIO	MEDIO	MEDIO	MEDIO	MEDIO	MEDIO	MEDIO	MEDIO	MEDIO
Programmazione, Progettazione interventi, Direzione dei lavori, esecuzione	●		●				●				
Gestire gli approvvigionamenti	●		●				●				●
Conferimento incarihi professionali											
Gestire accertamenti, morosità e decadenze			●								
Partecipazione a bandi di finanziamento e contributi. Richiesta di finanziamento e contributi	●		●								
Gestione delle gare di appalto.			●				●				
Gestire le Problematiche legali											
Gestire le infraastrutture		●									
Gestione della bollettazione e della fatturazione attiva			●				●		●		●
Gestire i Provvedimenti Amministrativi (richieste, volture, subentri, assegnazioni, consegne...)			●								
Gestire il protocollo			●								
Gestione amministrativa del personale.								●			
Gestire l'Amministrazione e la Contabilità							●		●		●
Elaborare il bilancio di esercizio							●		●		●
Gestione adempimenti societari e rapporti con gli Organi									●		
Gestione della salute e sicurezza nei luoghi di lavoro (processi contemplati dall'art. 30 del D.lgs. n. 81/08)								●			
Gestione rapporti contrattuali (con enti di certificazione, istituti di credito ecc.)			●								
Gestione adempimenti tributari											●
Selezione del personale			●								
Gestire il Patrimonio			●				●		●		●
Gestione risorse finanziarie			●				●				●
Gestione adempimenti in materia ambientale (nei cantieri)										●	
Gestire i Rapporti con P.A. in occasione di accertamenti, verifiche			●								

3) Valutazione dell'esposizione al rischio potenziale (rischio lordo)

Attraverso la metodologia illustrata, completata la mappatura dei processi e dei rischi di commissione di reati presupposto ad essi connessi, associati questi alle funzioni responsabili/coinvolte, si è giunti all'identificazione del relativo rischio potenziale (lordo) ovvero quel rischio, non insignificante o minimo, a cui, in assenza di controlli, è esposto il singolo soggetto apicale e quindi a cui è astrattamente esposto l'Impresa ai sensi del D.lgs. n. 231/01.

La valutazione del rischio lordo è stata condotta sulla base dello studio del contesto aziendale, delle interviste svolte ai responsabili di funzione, sull'analisi della documentazione messa a disposizione dalla Società. Le valutazioni del rischio sono espresse in termini qualitativi e sintetizzate poi a livello quantitativo, poichè questa metodologia di valutazione è stata considerata la più idonea a rappresentare il livello di rischio per processo/reato in base alle informazioni a disposizione.

Il metodo di valutazione del rischio utilizzato dall'Impresa è quello della "matrice di rischio". La "matrice del rischio", come mostra la sua rappresentazione seguente, ha lo scopo di individuare i principali scenari di rischio di un determinato sistema e di rappresentarli in un portafoglio di rischi potenziali (lordi) secondo le categorie della probabilità di accadimento e della gravità dell'impatto.



Nella matrice utilizzata, **la prima scala** concerne la gravità dell'impatto che potrebbe determinarsi a seguito della commissione di reati presupposto, individuata in funzione delle pene previste dal codice penale, delle corrispondenti quote (che esprimono la base di calcolo delle sanzioni) e della sanzione accessoria dell'interdizione, il tutto messo a sistema attraverso l'utilizzo di punteggi (fasce), in ordine crescente, come mostra la tabella che segue.

IMPATTO 1	Min quote	Max quote
SANZIONI	100	1000
fasce		
1	100	280
2	281	460
3	461	640
4	641	820
5	821	1000
IMPATTO 2	**Min (periodo)**	**Max (periodo)**
INTERDIZIONE	3	24
fasce		
1	3	7,2
2	7,2	11,4
3	11,4	15,6

4	15,6	19,8
5	19,8	24,0

Nell'allegato 1 sono riportati i livelli di gravità dell'impatto abbinati alle singole fattispecie di reato presupposto.

Nella matrice utilizzata, la seconda scala riguarda la probabilità di insorgenza.

Ad esclusione dei reati ricompresi tra quelli rilevanti ai fini del Piano della prevenzione della corruzione (elaborato a norma del PNA e della Delibera Anac n. 1134/17, in attuazione della Legge n. 190/12), oggetto questi di specifico *risk - assessement*, per gli altri reati rilevanti ai fini del D.lgs. n. 231/01, le valutazioni concernenti la probabilità di accadimento di un potenziale reato "presupposto" in uno specifico processo sono fondate sui fattori di seguito riportati, ai quali è stato attribuito un livello tra quelli in precedenza evidenziati, viene presa in considerazione anche la storia dell'Impresa.

Fattori del processo che incidono sulla probabilità di commissione del reato nel suo svolgimento.

Livello	FREQUENZA (su base annuale)	DISCREZIONALITA'	PRECEDENTI ACCADIMENTI	PROCCESSO NON COMPLESSO	AUTONOMIA ORG.VA U.O. RESPONSABILE
0,20	Raro	Scarsa	1 senza condanna	Molto complesso	Scarsa
0,40	sporadico	Ridotta	2 senza condanna	Abbastanza Complesso	Ridotta
0,60	frequente	media	3 senza condanna	Mediamente complesso	media
0,80	Molto frequente	Medio-alta	Almeno 1 con condanna non definitiva	Sufficientemente Complesso	Medio-alta
1,00	Ciclo continuo	Alta	Almeno 1 con condanna definitiva	Poco complesso	Alta
NA	Non applicabile	Non applicabile	Non applicabile	Non applicabile	Non applicabile

La probabilità di accadimento si valuta secondo una scala a cinque valori, applicati a ciascuno dei fattori che sono indicati successivamente, come mostrato di seguito:

PROBABILITA' PER SINGOLO FATTORE	Livello
BASSO	0,20
SUFFICIENTE	0,40
MEDIO	0,60
ALTO	0,80
MOLTO ALTO	1,00
	NA

PROBABILITA' COMPLESSIVA PER PROCESSO	Min	max
	0,2	5
fasce		
1	0,2	0,9
2	0,9	1,9
3	1,9	2,9
4	2,9	3,9
5	3,9	5,0

Dalla combinazione della gravità e della probabilità di accadimento, determinata quale prodotto arrotondato per eccesso della frequenza dei processi a rischio e della casistica storica di eventi dannosi, è emerso il "**LIVELLO DI RISCHIO POTENZIALE**" di commissione di reati presupposto nello svolgimento dei processi.

La definizione di "RISCHIO POTENZIALE" non implica che siano state rilevate oggettive predisposizioni a comportamenti illeciti. Piuttosto, tenuto conto delle fattispecie legali dei reati e dei *modus operandi* posti in luce nell'esperienza emergente dalla giurisprudenza, in rapporto con la modalità con cui la società sviluppa i processi aziendali, il "rischio", per ciascun parametro considerato, è stato collocato nella matrice e conseguentemente è stato attribuito un valore "sintetico" che esprime appunto il livello di rischio potenziale (confronta **Allegato 1**).

4) "AS IS" ANALYSIS

4.1. ANALISI DEL SISTEMA DI CONTROLLO INTERNO – SCI – ESISTENTE E VALUTAZIONE DELLA SUA AFFIDABILITA'.

L'attività di indagine è stata incentrata sulle caratteristiche **del Sistema di controllo** (*As is – analysis*) nelle sue componenti essenziali, di seguito indicate:

A. l'ambiente di controllo dell'Impresa ovvero il contesto aziendale nel quale vengono posti in essere i controlli stessi (misure di prevenzione a livello organizzativo e generale), misurato attraverso l'applicazione di *check-list*;
B. le attività di controllo interno ovvero i presidi specifici di controllo in uso.

Per verificare le carenze del "sistema di controllo interno" rispetto al contesto con le variabili di cui si compone sopra illustrato, ai fini della *compliance* al D.lgs. n. 231, si è proceduto preliminarmente, con l'ausilio di apposite *check-list*, all'esame (o se ne è verificata l'esistenza/la non sussistenza) della documentazione necessaria a comprenderne le caratteristiche ed in particolare:

- Statuto;
- Struttura organizzativa complessiva (organigramma);
- Articolazione dei ruoli e delle funzioni (funzionigramma);
- Sistema di deleghe e procure risultante da visura camerale;
- Sistemi di pianificazione, *reporting* e *controlling;*
- Manuali / Regolamenti e documenti interni di raccolta di procedure operative, gestionali, di qualità e di sicurezza;
- Procedure e protocolli formalizzate.

Relativamente alle attività di controllo interno ovvero ai presidi specifici di controllo in uso, di seguito viene illustrata la metodologia utilizzata per la valutazione della loro adeguatezza in termini di capacità di risposta al rischio.
In sintesi le componenti **del Sistema di Controllo Interno (SCI)** sono stati ricondotti ai seguenti elementi.

Elementi del sistema di controllo interno

DELECHE E PROCURE	MISURE ORG.VE	SEGREGAZIONE COMPITI	TRACCIABILITA'	SISTEMA DI CONTROLLO

Tali componenti (**elementi del Sistema di Controllo Interno – SCI)** che nel loro insieme devono integrarsi organicamente in un'architettura del sistema che rispetti una serie di principi di controllo, sono state analizzate e valutate in rapporto alle *best-*

practices (attraverso la *Gap-analysis*), avendo come riferimento nell'imputazione di valori non la loro efficace applicazione o conformità a norme imperative bensì la loro esistenza e aderenza al dettato del D.lgs. n. 231/01.

Il sistema di controllo interno, è stata esaminato in termini di "affidabilità" ovvero di livello di debolezza aziendale potenziale; le non conformità possono essere sfruttate per commettere Reati e consistono nella mancanza di misure preventive o in un clima etico aziendale negativo.

La non conformità potenziale è tanto più forte quanto minore è la "copertura" ovvero la l'esistenza di elementi del sistema di controllo interno nel contrastare il compimento di reati e quindi in definitiva di ridurre la probabilità di accadimento, come mostra la seguente tabella, utilizzata ai fini dell'analisi.

Determinazione del livello di conformità degli elementi del SCI

Livello di affidabilità	
NC	-
0,20	BASSO
0,40	SUFFICIENTE
0,60	MEDIO
0,80	ALTO
1,00	MOLTO ALTO

Ne consegue che il predetto sistema di controllo preventivo è ADEGUATO se è in grado di:

• escludere che un qualunque soggetto operante all'interno dell'ente possa giustificare la propria condotta adducendo l'ignoranza delle direttive aziendali;

• evitare che, nella normalità dei casi, il reato possa essere causato dall'errore umano (dovuto a imprudenza, negligenza o imperizia) nella valutazione delle direttive aziendali.

Ciò anche in considerazione del fatto che i reati in relazione ai quali si può ravvisare la responsabilità dell'ente sono, per lo più, di tipo delittuoso e perseguiti a titolo doloso e che l'aggiramento dei modelli non può avvenire per mera negligenza o imperizia, ma unicamente per previsione e volontà dell'evento.

Inoltre i controlli interni devono essere implementati in modo tale da garantire in massimo grado l'adempimento degli obblighi di direzione o vigilanza.

Nell'**allegato 1** è stata fornita l'evidenza dei risultati della valutazione degli elementi specifici di controllo interno sopra esaminati, espressa in termini di loro affidabilità per singolo processo/attività sensibile.

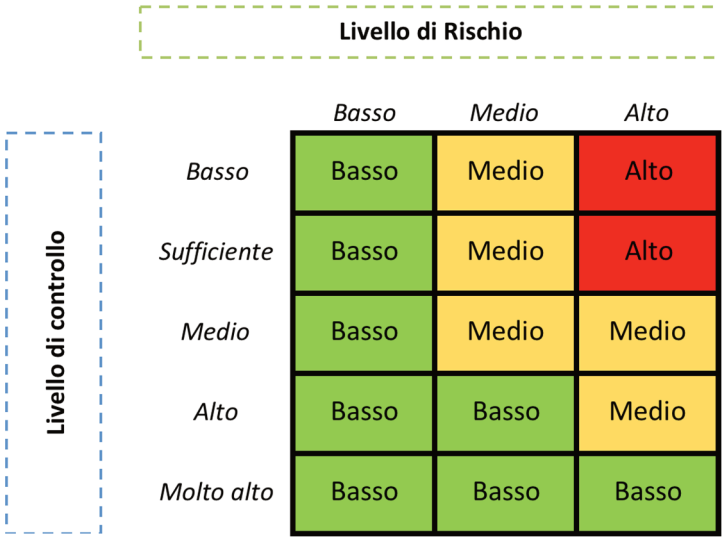
4.2. DETERMINAZIONE DEL RISCHIO RESIDUO SULLA BASE DELL'AFFIDABILITA' DEL SCI

Il livello della vulnerabilità è stato quindi determinato in funzione della presenza e dell'efficacia, per ciascun processo e attività sensibile, delle misure di mitigazione dei rischi.

I parametri sopra indicati, sono stati pertanto successivamente messi in relazione con il livello di rischio potenziale, calcolato come illustrato nei paragrafi che precedono, secondo la matrice di correlazione di seguito riportata, per addivenire alla determinazione del livello di rischio residuo per ciascun processo in essa indicato.

Correlazione livello di rischio potenziale / grado di affidabilità dei controlli	Rischio residuo
Livello di Rischio Basso e Grado di Controllo Basso	Basso
Livello di Rischio Basso e Grado di Controllo Sufficiente	Basso
Livello di Rischio Basso e Grado di Controllo Medio	Basso
Livello di Rischio Basso e Grado di Controllo Alto	Basso
Livello di Rischio Basso e Grado di Controllo Molto alto	Basso
Livello di Rischio Medio e Grado di Controllo Basso	Medio
Livello di Rischio Medio e Grado di Controllo Sufficiente	Medio
Livello di Rischio Medio e Grado di Controllo Medio	Medio
Livello di Rischio Medio e Grado di Controllo Alto	Basso
Livello di Rischio Medio e Grado di Controllo Molto alto	Basso
Livello di Rischio Elevato e Grado di Controllo Basso	Alto
Livello di Rischio Elevato e Grado di Controllo Sufficiente	Alto
Livello di Rischio Elevato e Grado di Controllo Medio	Medio
Livello di Rischio Elevato e Grado di Controllo Alto	Medio
Livello di Rischio Elevato e Grado di Controllo Molto alto	Basso

I risultati ottenuti con l'applicazione della matrice, come mostrato dalla tabella seguente, per ciascun processo, sono contenuti nell'**Allegato 1**.



8. RISK MITIGATION

8.1. Gap Analysis

A conclusione della analisi e valutazioni del **SCI (sistema di controllo interno)** è stata condotta la "*gap analisys*", i cui risultati sono contenuti nell'**Allegato 1**, attraverso la quale sono state individuate le azioni correttive necessarie a portare o contenere il "rischio residuo" all'interno della soglia ritenuta "accettabile" ovvero contenuta nel livello "BASSO".

È stata pertanto posta in essere l'analisi degli scostamenti tra il modello di prevenzione ottimale e l'attuale sistema di controlli e le procedure esistenti (*As is analisys)*. In altri termini, si è operata una comparazione tra il sistema di controlli "così com'è" ed il "come dovrebbe essere". Ciò ha consentito di individuare le azioni correttive necessarie a contenere il rischio residuo all'interno della soglia di "accettabilità" e comunque di ridurlo ulteriormente, attraverso una ponderazione basata sul rapporto costi-benefici operato in relazione ai *gap* individuati rispetto agli standard.

Sono state pertanto individuate, nell'ambito dell'attività di *Risk Management*, delle misure di *risk response*. improntate:

- A ridimensionare e mitigare il rischio (*risk mitigation*) _ ridurre il rischio significa porre in essere azioni mirate a limitarne la frequenza e/o l'impatto, portando l'esposizione al di sotto della soglia di accettabilità. Il modo più comune di realizzare tale "risposta" consiste nell'introdurre un certo numero di misure di

controllo volte a ridurre sia la probabilità che l'evento avverso possa accadere, sia gli effetti negativi nel caso in cui il reato dovesse effettivamente verificarsi;

Tale attività è stata effettuata tenendo conto, per ciascun processo, sulla base del livello di rischio residuo, dei seguenti fabbisogni di intervento "mitigativo", in taluni casi innalzati al livello superiore prudenzialmente e discrezionalmente.

Livello di rischio residuo	Interventi da attivare:
Basso	**Fascia VERDE – indice di intervento BASSO**. Appare necessario e sufficiente il presidio operato attraverso le prescrizioni/norme di comportamento contenute nel Modello, nelle Parti Speciali, nel Codice etico e sanzionatorio e quindi la loro implementazione ed efficace attuazione, con particolare attenzione all'attività dell'OdV tesa alla vigilanza sull'efficace attuazione del Mog. e al miglioramento continuo.
Medio	**Fascia GIALLA – indice di intervento MEDIO**. Situazione che richiede l'individuazione e la programmazione nel medio periodo di azioni di miglioramento sul sistema di controllo interno oltre che assicurare l'implementazione ed efficace attuazione del Modello.
Alto	**Fascia ROSSA – indice di intervento ALTO**: Situazione da gestire attraverso un programma di attività specifiche per fattispecie di reato, da individuare con la *gap analisys,* da attuare nel breve periodo attraverso l'inserimento di appositi presidi a livello strutturale (deleghe e procure, organigramma ecc). Nondimeno è necessaria l'implementazione ed efficace attuazione del Modello ma auspicabilmente dopo aver apportato al sistema organizzativo le necessarie modifiche strutturali.

Nell'ambito di tali attività di *risk response,* sulla base della *gap analisys,* è stato pertanto elaborato l'*action plan* per i processi per i quali il rischio residuo è risultato non BASSO.

8.2. Action Plan

Si tratta di elaborare un "piano di gestione del rischio", descrivendo le criticità e le azioni correttive per programmarle nell'ottica di una mitigazione nel tempo del rischio non accettabile sulla base di quanto emerso ad esito della *gap-analisys*.
Nello specifico, le principali raccomandazioni formulate in relazione alle criticità emerse sulla base della *gap-analisys,* sono riconducibili ad un RISCHIO BASSO il cui contenimento entro soglie di accettabilità passa attraverso le azioni già svolte e sinteticamente riportate nella tabella che segue.

Livello di rischio residuo	Interventi da attivare:
Basso	**Fascia VERDE – indice di intervento BASSO**. Appare necessario e sufficiente il presidio operato attraverso le prescrizioni/norme di comportamento

	contenute nel Modello, nelle Parti Speciali, nel Codice etico e sanzionatorio e quindi la loro implementazione ed efficace attuazione;

9. RISCHIO RESIDUO IN RELAZIONE A QUELLO ACCETTABILE DOPO LA GAP ANALISYS

Complessivamente, possiamo ritenere che il livello di "rischio netto" o "residuo" di S.E.PI. S.p.A. dopo l'attuazione dell'*action plan*, si attesti, alla luce delle analisi svolte, ad un livello **BASSO** e quindi **ACCETTABILE**, ovvero contenuto entro la soglia della tollerabilità così come in precedenza definita per lo specifico contesto in cui si posiziona ed opera l'Impresa.