Terna

LG058

Global Compliance Program

19/12/2025

LINEE GUIDA

Approvato

Giuseppina Di Foggia
(**Amministratore Delegato**)

Storia delle revisioni

Rev. 04 del 18/12/2025	*Quinta emissione che ha previsto l'ampliamento dello scopo del Global Compliance Program al fine di soddisfare gli obblighi di rendicontazione in ambito sostenibilità; l'aggiornamento delle regole di diffusione del sistema di controllo interno di Terna verso le Società Estere del Gruppo; la revisione dei processi e delle aree a rischio con introduzione di nuove aree rilevanti in ottica di Sostenibilità; l'aggiornamento della Governance di Compliance e l'eliminazione del COB, la revisione delle regole di ingaggio del Compliance Officer in caso di segnalazioni Whistleblowing; la rivisitazione delle regole di formazione sul Global Compliance Program; la creazione di una nuova Appendice C e l'aggiornamento dei flussi di cui all'Appendice B.*
Rev. 03 del 14/12/2023	*Quarta emissione che ha previsto l'adeguamento del Global Compliance Program alle novità introdotte dalla LG054 Whistleblowing in materia di segnalazioni e modifica della composizione del Compliance Officer Bureau (COB)*
Rev. 02 del 02/09/2022	*Terza emissione che ha previsto la revisione della struttura del Global Compliance Program per adeguarlo alle principali e più recenti best practice e normative applicabili in materia di compliance program, individuate a titolo esemplificativo nel par. 3.2. del Global Compliance Program.* *Adeguamento del documento seguendo il c.d. "approccio per processi", individuando e regolando i macro-processi aziendali rilevanti a livello di Gruppo, emersi nei risk assessment in ambito di corporate liability (in precedenza il GCP era strutturato per categorie di reati astrattamente rilevanti per il Gruppo) ciò al fine di rendere il GCP più coerente con le predette best practice e con i modelli di compliance da ultimo adottati dal Gruppo (i.e. Modelli di Organizzazione, Gestione e Controllo ai sensi del D. Lgs. 231/2001) e per meglio riflettere l'organizzazione delle società del Gruppo, nonché agevolare la comprensione del GCP da parte dei Destinatari*
Rev. 01 del 18/12/2019	*Seconda emissione*
Rev. 00 del 10/11/2017	*Prima emissione*

Sistemi di Gestione e/o Modelli Organizzativi di riferimento

	Sistemi di Gestione certificati/accreditati
☑	***SGQ*** *(Qualità)*
☐	***SGA*** *(Ambiente)*
☐	***SGSL*** *(Sicurezza e Salute sui luoghi di Lavoro)*
☐	***SGPIR*** *(Prev. Incidenti Rilevanti – Direttiva Seveso)*
☐	***SGSI*** *(Sicurezza delle Informazioni)*
☐	***SGE*** *(Energia consumata per usi propri)*
☐	***SGQ LST*** *(Laboratorio LST)*
☐	***SGQ TAR*** *(Centro di Taratura)*
☑	***SGAC*** *(Anticorruzione)*
☐	***SGAM*** *(Gestione Asset)*
☐	***SGPCI*** *(Prev. e Controllo Infezioni – Biosafety)*
☑	***SGC*** *(Compliance)*
☐	***SGPG*** *(Parità di Genere)*
☐	***SGPAC*** *(Processi Amministrativi e Contabili)*

	Modelli Organizzativi
☐	***BCM*** *(Business Continuity Model)*
☐	***TCM*** *(Tax Compliance Model)*
☐	***PRV*** *(Modello Privacy)*
☐	***M262*** *(Modello 262)*
☐	***M231*** *(Modello 231)*
☐	***MIMP*** *(Modello Imparzialità)*
☐	***SCIIS*** *(Sist. Controllo Informativa di Sostenibilità)*

(Per approfondimenti sui Sistemi di Gestione certificati/accreditati, clicca gui)

Indice

1. Generalità

La Capogruppo TERNA - Rete Elettrica Nazionale Società per Azioni ("**TERNA**") è la società responsabile in Italia della trasmissione e del dispacciamento dell'energia elettrica sulla rete ad alta e altissima tensione. Le sue azioni sono quotate sul Mercato italiano della Borsa Telematica organizzato e gestito da Borsa Italiana S.p.A., segmento Mercato Telematico Azionario ("MTA"), comprendente le imprese di media e grande capitalizzazione e allineato alle *best practice* internazionali e appartenenti all'indice Financial Times Stock Exchange - Milano Indice di Borsa (FTSE MIB). TERNA inoltre è tra i grandi emittenti italiani quotati presenti nell'indice MIB 40 ESG, il primo indice blue-chip per l'Italia dedicato alle best practice ambientali, sociali e di governance (ESG) che combina la misurazione della performance economica con valutazioni ESG in linea con i principi del Global Compact delle Nazioni Unite.

TERNA è la *holding* di un gruppo multinazionale che opera in un settore complesso e ampiamente regolamentato e in ambienti economici, politici, sociali e culturali estremamente variegati (il "**Gruppo Terna**").

2. Scopo del documento

In molti Paesi esteri in cui opera il Gruppo Terna esiste un regime di responsabilità penale o assimilabile, suscettibile di applicazione alle persone giuridiche in relazione a comportamenti illeciti commessi da rappresentanti, dipendenti o soggetti terzi che agiscono nel loro interesse.

La maggior parte di tali normative estere incoraggia le aziende a dotarsi di strumenti di governo societario e sistemi di mitigazione dei rischi, volti a prevenire la commissione di reati da parte di tali soggetti, prevedendo, in alcuni casi, un'esenzione o una mitigazione delle sanzioni applicabili qualora vengano adottate ed efficacemente attuate adeguate misure di prevenzione.

Inoltre, la transnazionalità di talune fattispecie di illeciti può comportare profili specifici di potenziale pericolosità anche per la Capogruppo per gli illeciti commessi nell'interesse o vantaggio della stessa da parte delle Società Estere.

Il Global Compliance Program, adottato da Terna sin dal 10 novembre 2017 e con successivi aggiornamenti, costituisce un presidio volto ad armonizzare gli sforzi delle Società Estere nel prevenire la responsabilità penale aziendale fornendo alle stesse un approccio condiviso, coerente e uniforme contro possibili comportamenti illeciti ed è ispirato alle principali normative e *best practice* internazionali applicabili in materia di corporate liability.

Il GCP in tale contesto mira a (i) definire gli Standard generali di controllo e i Principi di Comportamento applicabili ai dipendenti, agli amministratori e agli altri membri degli organi di gestione e di controllo delle SE ("Esponenti Aziendali") nonché, ove applicabili, ai Terzi e agli Altri Destinatari, al fine di prevenire la commissione di fattispecie di reato rilevanti, e (ii) ad assicurare la divulgazione verso le Società Estere e il monitoraggio dell'attuazione degli atti di indirizzo di Terna anche in funzione dell'accountability richiesta dalle normative europee in tema di sostenibilità.
Il GCP costituisce, al pari della normativa di cui all'Appendice C - a03LG058, un atto di indirizzo di TERNA la cui applicazione è rivolta alle Società Estere chiamate a recepirlo; laddove opportuno o

richiesto dalla normativa locale applicabile, ciascuna Società Estera definisce e adotta altresì dei propri Compliance Program Locali e procedure deliberate a livello locale, in conformità con la suddetta normativa e in linea con quanto previsto dal presente GCP; tali programmi sono quindi riportati nell'ambito dell'Allegato Paese di riferimento approvato da ciascuna Società Estera.
Dunque, in tali contesti, l'Allegato Paese integra il GCP, recepito dalle SE secondo quanto specificato al par.6.1, con le regole eventualmente previste dai Compliance Program Locali.

Le società italiane controllanti le Società Estere adottano il GCP con lo scopo di dotare esse stesse, le loro controllate di un indirizzo del socio di controllo fornendo un indirizzo comune a dette controllate per contrastare più efficacemente fenomeni di criminalità di impresa.

3. Riferimenti Esterni

Il GCP si ispira alle più importanti normative e *best practice* anche internazionali tra cui, a titolo esemplificativo e non esaustivo, si annoverano le seguenti:

(i) il Decreto Legislativo dell'8/06/2001, n. 231 ("**Decreto 231**") e successivi aggiornamenti, che disciplina il regime di responsabilità amministrativa (simile a una responsabilità penale) delle persone giuridiche risultante dalla commissione di determinati reati per conto o nell'interesse delle stesse;

(ii) il "Codice di Corporate Governance" delle società quotate promosso da Borsa Italiana S.p.A.

(iii) le *Federal Sentencing Guidelines Manual & Supplement*, adottate dalla United States Sentencing Commission il 1° novembre 2010;

(iv) Foreign Corruption Practice Act ("**FCPA**") del 1977 e successivi aggiornamenti;

(v) la "*Resource Guide to the U.S. Foreign Corrupt Practices Act"* emanata dal Criminal Division of the U.S. Department of Justice ("**DOJ**") e dall'Enforcement Division of the U.S. Securities and Exchange Commission del 2012 e successivi aggiornamenti;

(vi) UK Bribery Act del 2010 e successivi aggiornamenti;

(vii) *Loi Sapin II*, introdotta con Legge n. 2016-1691 in materia di trasparenza, lotta alla corruzione e modernizzazione della vita economica, pubblicata il 9 dicembre 2016;

(viii) la *Good Practise Guidance on Internal Controls, Ethics, and Compliance* adottata dal Consiglio dell'OCSE il 18 febbraio 2010;

(ix) la "*Resource Guide to the U.S. Foreign Corrupt Practices Act"* emanata dal Criminal Division of the U.S. Department of Justice ("**DOJ**") e dall'Enforcement Division of the U.S. Securities and Exchange Commission del 2012 e successivi aggiornamenti;

(x) *ICC Rules on Combatting Corruption*, pubblicato dalla Camera di Commercio Internazionale (ICC), edizione 2023;

(xi) *la "The OECD 2021 Recommendation for Further Combating Bribery of Foreign Public Officials in International Business Transactions" del novembre 2021;*

(xii) l'"*Evaluation of Corporate Compliance Programs*" del DOJ del 2017 e successivi aggiornamenti;

(xiii) l'*Anti-Corruption Ethics and Compliance Programme for Business: A Practical Guide* adottato dall'United Nations Office on Drugs and Crime (UNODC) nel settembre del 2013;

(xiv) le raccomandazioni adottate dalla Financial Action Task Force – Gruppo d'Azione Finanziaria Internazionale ("**FATF-GAFI**" o "**GAFI**") sul riciclaggio e sul finanziamento del terrorismo del 2012 e successivi aggiornamenti;

(xv) i regolamenti europei in materia di riciclaggio, ricerca, sequestro e confisca dei proventi da reato e sul finanziamento del terrorismo (tra cui la Direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio, del 20 maggio 2015 e il regolamento delegato (UE) 2016/1675 e successivi aggiornamenti);

(xvi) il D.Lgs. 10 marzo 2023 n. 24, in attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali;

(xvii) la Direttiva (UE) 2019/1937 del Parlamento Europeo e del Consiglio del 23 ottobre 2019 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione.

4. Definizioni e Abbreviazioni

Action Plan: piano di interventi finalizzati al miglioramento del sistema di controllo, individuato tenendo in considerazione gli esiti del Risk Assessment e la strategia di Risk Management definita per il Rischio (evitare, ridurre, accettare e monitorare e trasferire).

Allegato Paese: il documento predisposto in ciascuna Società Estera che recepisce i dettami del GCP e descrive i Compliance Program Locali e le procedure dalla stessa adottate a livello locale.

Aree a Rischio: le aree di attività nel cui ambito può considerarsi, in termini più concreti, il rischio di commissione dei Reati.

ASC-ASCO: struttura Affari Societari Controllate nell'ambito di Affari Societari e Corporate Governance di Terna S.p.A.

HSEQ-DOC: struttura Presidio Documentale nell'ambito di HSE Qualità e Rischi di Terna S.p.A.

Bribery Act: Bribery Act del Regno Unito del 2010.

CMP-PCR: struttura Presidio Corporate Liability e Compliance Risk nell'ambito di Compliance di Terna S.p.A.

Codice Etico: il codice etico adottato nell'ambito del Gruppo Terna e approvato dal Consiglio di Amministrazione di TERNA il 21 maggio 2002 e relativi aggiornamenti, volto a definire i principi etico-comportamentali ai quali gli Amministratori, i Dipendenti e tutti coloro che operano in nome e per conto di TERNA o delle società del Gruppo Terna devono attenersi.

Compliance Officer o CO: soggetto individuato in ciascuna società Estera con delibera dell'Organo Amministrativo della stessa, deputato ad implementare e a dare esecuzione agli indirizzi della Capogruppo derivanti dal GCP in materia di Compliance. Il Compliance Officer è inoltre deputato ad implementare i Compliance Program Locali che dovessero essere richiesti dalle singole normative applicabili in materia di Corporate Liability ponendosi quale punto di riferimento per la Compliance della società Estera.

Compliance Program Locali: programmi di compliance volti a prevenire la *corporate liability* adottati dalle società Estere ai sensi della normativa locale applicabile nel Paese di riferimento e in linea con gli Standard Generali di Controllo e i Principi di Comportamento previsti dal Global Compliance Program.

Decreto 231: il D.lgs. 8 giugno 2001 n. 231, recante la "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300*" e successive modifiche e integrazioni.

Destinatari: gli Esponenti Aziendali e gli Altri Destinatari.

DOJ: il U.S. Department of Justice.

Due Diligence: processo organizzato di raccolta e di analisi di informazioni dettagliate di varia natura sulle Terze Parti svolto dalle diverse strutture competenti in relazione all'istaurazione, mantenimento e conclusione di rapporti contrattuali/commerciali con le stesse oppure con riferimento ad una specifica operazione, finalizzato a verificare il rispetto dei principi etici, anticorruzione e antiriciclaggio stabiliti da Terna.

Esponenti Aziendali: i dipendenti, gli amministratori e gli altri membri degli organi di gestione e di controllo delle società Estere.

Facilitation Payments: indica i pagamenti fatti allo scopo di accelerare o garantire l'effettuazione di un'attività nell'esercizio di una funzione pubblica considerata di routine (per esempio, concessione di un permesso di soggiorno, concessione di un servizio di protezione da parte delle forze di polizia, organizzazione di un'attività ispettiva, concessione di una licenza commerciale, formalità connesse a operazioni di carico e scarico di merce).

FATF-GAFI o **GAFI:** Financial Action Task Force – Gruppo di Azione Finanziaria Internazionale[1] (organismo che coordina la lotta contro il riciclaggio di denaro e il finanziamento del terrorismo).

FCPA: Foreign Corruption Practice Act degli Stati Uniti d'America del 1977 e successivi aggiornamenti.

Funzionario Pubblico: (a) qualunque funzionario, eletto o nominato, che esercita una pubblica funzione legislativa, amministrativa o giudiziaria; (b) qualunque persona che svolge funzioni pubbliche in qualsiasi ramo del governo nazionale, regionale o comunale o che esercita una funzione pubblica per qualsiasi agenzia o impresa pubblica, come i funzionari che esercitano funzioni pubbliche in imprese statali.

Global Compliance Program o GCP: il presente Global Compliance Program, documento adottato da TERNA in data 10 novembre 2017 e dalle società Estere e sue successive modifiche.

Gestore: il/i soggetto/i, individuati dalla società, competenti per la gestione delle segnalazioni Whistleblowing.

Gruppo Terna: TERNA S.p.A. e le altre società dalla medesima controllate ai sensi dell'art. 93 del Decreto Legislativo 24 febbraio 1998, n. 58 (c.d. Testo Unico della Finanza).

Linee Guida Anticorruzione o **LG059*:*** le linee guida Anticorruzione adottate dal Consiglio di Amministrazione di TERNA elaborate tenendo conto delle principali convenzioni internazionali, della normativa comunitaria, del FCPA e del Bribery Act in tema di prevenzione e lotta alla corruzione. Tali linee guida contengono principi e regole di comportamento per tutti gli Esponenti Aziendali (di tutte le società del Gruppo così come per qualsiasi terzo che agisca in nome e/o per conto di TERNA o del Gruppo Terna, quali fornitori, agenti, consulenti, partner commerciali o qualsiasi altra controparte.

Linea Guida Whistleblowing o LG054: la Linea Guida adottata da TERNA in materia di Whistleblowing.

Liste: per Liste si intendono

i. le liste Paesi a rischio corruzione (ad es. indice di percezione della corruzione di Transparency International);

ii. elenchi di soggetti (persone fisiche e/o giuridiche) predisposti dall'Unione Europea, da ogni singolo Stato membro dell'Unione Europea, dal Regno Unito, dagli Stati Uniti d'America, dalle Nazioni Unite e da ogni altra giurisdizione, e rilevanti – ai sensi della normativa applicabile o per effetto di disposizioni contrattuali, come di volta in volta aggiornate, integrate, modificate ed efficaci – per TERNA e le società del Gruppo Terna, che contengono gli elementi di identificazione dei soggetti (persone fisiche e/o giuridiche) ed attività con i quali, o in relazione

[1] Il Gruppo d'azione finanziaria internazionale (GAFI) è un organismo internazionale il cui obiettivo è elaborare e promuovere strategie di lotta contro il riciclaggio di denaro e il finanziamento del terrorismo e della proliferazione delle armi di distruzione di massa. (v. http://www.dt.mef.gov.it/it/attivita_istituzionali/rapporti_finanziari_internazionali/organismi_internazionali/gafi/

alle quali, è vietato effettuare, direttamente o indirettamente, operazioni, in quanto soggetti a Misure Restrittive;

iii. lista Paesi a rischio riciclaggio e finanziamento al terrorismo elaborate dall'UE, liste «black list» /«grey list» (indicate da GAFI[2], UE, ecc.), liste ONU relative alle sanzioni finanziarie applicate a soggetti ed entità collegati alle organizzazioni terroristiche.

Local Compliance Assistant: soggetto eventualmente nominato nell'ambito della singola Società Estera, con delibera dell'Organo Amministrativo della stessa e con parere positivo del CO della Società Estera, deputato, quale presidio locale, ad assistere quest'ultimo nell'esecuzione dei propri compiti e incaricato di raccogliere informazioni, segnalare eventuali criticità e interfacciarsi con il CO e la struttura CMP-PCR.

Management Locale: l'amministratore delegato o l'executive director o il componente dell'Organo Amministrativo con deleghe operative o funzione corrispondente.

Misure Restrittive: restrizioni commerciali e finanziarie adottate dall'Unione Europea, da ogni singolo Stato membro dell'Unione Europea, dal Regno Unito, dagli Stati Uniti d'America, dalle Nazioni Unite e da ogni altra giurisdizione, e rilevanti – ai sensi della normativa applicabile o per effetto di disposizioni contrattuali, come di volta in volta aggiornate, integrate, modificate ed efficaci – per TERNA e le società del Gruppo Terna nei confronti di Paesi terzi e/o di soggetti (persone fisiche e/o giuridiche) e/o di beni e servizi (inclusi software, tecnologie, engineering e assistenza tecnica) e attività.

Organo Amministrativo: Consiglio di amministrazione o organismo o funzione corrispondente delle società Estere.

Pubblica Amministrazione o **P.A.** o **Ente pubblico:** ciascuno degli enti o apparati che concorrono all'esercizio delle funzioni legislativa, amministrativa o giudiziaria di un singolo stato, ivi compresi gli enti governativi.

RU: Direzione Risorse Umane di Terna S.p.A.

Principi di Comportamento: gli standard minimi di comportamento connessi alle Aree a Rischio.

Processi: i macro-processi rilevanti, individuati dal GCP, nell'ambito dei quali vengono individuate le Aree a Rischio.

Reati: determinati tipi di comportamenti illeciti qualificabili come reati in diverse giurisdizioni e che potrebbero essere potenzialmente commessi da un Esponente Aziendale o da un Terzo e la cui prevenzione nel Gruppo deve essere considerata una priorità al fine di gestire il proprio business con onestà e integrità. L'elenco dei Reati è individuato al par. 13.4 del Global Compliance Program e dettagliato nell' Appendice A - a01LG058.

[2] https://www.bancaditalia.it/compiti/supervisione-normativa-antiriciclaggio/comunicazioni/liste-gafi/?dotcache=refresh

Red Flag: uno o più indicatori di anomalia/fattori di Rischio Potenziale (sotto il profilo della corruzione, riciclaggio o ulteriori fattispecie di reato rilevanti) che devono essere verificati nell'ambito della Due Diligence.

Rischio: qualsiasi evento futuro che nell'ambito dell'azienda, da solo o in correlazione con altri eventi interni o esterni, può influenzare negativamente il raggiungimento degli obiettivi indicati nelle normative di riferimento del singolo Paese.

Rischio Potenziale: la possibilità che un evento futuro e incerto in una specifica area/processo aziendale realizzi un Rischio.

Rischio Residuo: il Rischio di Reati connesso a una specifica area/processo aziendale mitigato dall'esistenza ed effettività dei controlli interni adottati.

Risk Assessment: l'analisi dei processi aziendali volta a identificare e valutare i potenziali rischi di commissione delle fattispecie di Reati rilevanti ed i relativi presidi esistenti.

OHP-ORG: la struttura Organizzazione, Processi e Policy nell'ambito di Organizzazione HRIS & Policy di Terna S.p.A.

Sistema di Controllo Interno e di Gestione dei Rischi o **SCIGR:** insieme della cultura, delle capacità, delle regole, procedure e delle pratiche aziendali, nonché delle strutture organizzative, volte a definire un sistema di accountability per l'identificazione, misurazione, gestione, mitigazione e controllo dei principali rischi a livello di Gruppo, mantenendo di conseguenza alta la fiducia degli stakeholders con riguardo al governo e al controllo del Gruppo medesimo.

Società Estera/e/o SE: società non italiana/e del Gruppo Terna.

Standard Generali di Controllo: standard generali di controllo individuati e disciplinati dal GCP che ciascuna Società Estera deve adottare in coerenza con il SCIGR adottato dal Gruppo Terna volti a consentire, attraverso un adeguato processo di identificazione, misurazione, gestione e monitoraggio dei principali rischi, una conduzione dell'impresa sana, corretta e coerente con gli obiettivi prefissati.

TERNA: la Capogruppo TERNA - Rete Elettrica Nazionale Società per Azioni (in forma abbreviata TERNA S.p.A.).

Terzi o Altri Destinatari: qualsiasi terzo che agisca in nome e/o per conto di una SE, quali fornitori, agenti, consulenti, partner commerciali o qualsiasi altra controparte.

5. Top Level Commitment

Il Gruppo Terna conduce il proprio business secondo i criteri di lealtà, legalità, correttezza, integrità e trasparenza, nel rispetto delle normative applicabili in Italia e all'estero in materia di *Criminal Corporate Liability*.

Il Gruppo Terna promuove e diffonde una cultura etica e di compliance. L'impegno è assunto, principalmente, da tutti i vertici del Gruppo Terna (Top-Level Commitment) che si adoperano per diffondere tale messaggio a tutti i livelli.
A tale scopo, i vertici delle singole società del Gruppo Terna definiscono e diffondono linee guida, procedure e politiche interne volte a regolare e formalizzare detto impegno al fine di prevenire la commissione di attività illecite.
In particolare, anche gli organi amministrativi delle Società Estere esprimono, e sono chiamati a diffondere in modo chiaro, il messaggio di assoluta osservanza dei principi di etica, integrità e legalità del Gruppo Terna.

6. Struttura del Global Compliance Program

Il presente documento, oltre a esplicitare l'impegno del top management nella promozione e definizione di una cultura etica e di compliance (cd. top level commitment), nonché le modalità di adozione, implementazione e successive modifiche del GCP da attuare anche in ciascuna Società Estera, individua e disciplina[3]:

- le modalità di Risk Assessment, descritte al par. 7, necessarie per la valutazione dell'esposizione al rischio di commissione dei Reati identificati all'interno del presente GCP e che costituisce la base per la predisposizione dell'Allegato Paese e dei Compliance Program Locali;
- gli standard generali di controllo ("Standard Generali di Controllo"), descritti al par. 13.2, che ciascuna Società Estera deve adottare, in coerenza con il Sistema di Controllo Interno e Gestione dei Rischi di cui al par. 13.1, volti a consentire, attraverso un adeguato processo di identificazione, misurazione, gestione e monitoraggio dei principali rischi, una conduzione dell'impresa sana, corretta e coerente con gli obiettivi prefissati;
- i ruoli del Compliance Officer e di PCR descritti nei par. 8 e successivi, individuati quali figure preposte a garantire la diffusione della conoscenza ed agevolare il funzionamento del Global Compliance Program e dell'Allegato Paese di riferimento e degli eventuali ulteriori Compliance Program locali;
- i Processi rilevanti e le Aree a Rischio nel cui ambito potrebbe astrattamente sussistere il rischio di commissione dei Reati individuati dal GCP e che potrebbero essere potenzialmente commessi da un Esponente Aziendale o da un Terzo e la cui prevenzione nel Gruppo deve essere considerata una priorità al fine di gestire il proprio business con onestà e integrità. Per ogni macro-processo sono individuati gli standard di comportamento minimi connessi alle Aree a Rischio (i "Principi di Comportamento"). I Processi descritti costituiscono la base di riferimento per ciascuna Società Estera per l'elaborazione, attraverso specifica attività di Risk Assessment, del rispettivo Allegato Paese. I Principi di Comportamento di cui al par. 14 devono intendersi applicabili trasversalmente per tutti i Processi e le Aree a rischio disciplinati nel Global Compliance Program;

[3] La stuttura del GCP è basata sulle principali best practice e normative applicabili in materia di compliance program. Per quanto concerne l'individuazione dei Processi e delle Aree a Rischio, questa è stata effettuata tenendo in considerazione i macro-processi e le macroaree di rischio rilevanti a livello del Gruppo Terna.

- la formazione agli Esponenti Aziendali e l'informazione dei Destinatari in ordine al GCP per garantire l'effettiva applicazione dei presidi definiti, come indicato al par. 9;
- il sistema di whistleblowing per la gestione delle segnalazioni di comportamenti illeciti o irregolarità e di reporting interno, riportati al par. 10;
- i presidi per il monitoraggio e il miglioramento continuo del GCP, disciplinati al par. 11;
- il sistema sanzionatorio applicabile in caso di violazione delle disposizioni individuate nell'ambito del GCP e che deve essere tenuto in considerazione dalle Società Estere nell'ambito dei propri Compliance Program Locali, disciplinati al par. 12.

6.1 Adozione del GCP, implementazione e successive modifiche

Il GCP è stato approvato dal Consiglio di Amministrazione di TERNA[4] ed esprime i principi che rientrano tra i valori fondamentali del Gruppo Terna e che ne ispirano l'organizzazione e le attività, anche in attuazione dei principi del Codice Etico comuni alle Società Estere; eventuali successive modifiche al GCP sono approvate dall'Amministratore Delegato di TERNA in virtù della delega conferita dal Consiglio di Amministrazione in sede di approvazione del GCP[5].

TERNA, anche per il tramite delle proprie controllate di diritto italiano[6], promuove pertanto l'adozione del GCP verso ciascuna Società Estera direttamente controllata che, a sua volta, è chiamata a recepire ed approvare il GCP (e ogni relativo aggiornamento) con delibera del proprio Organo Amministrativo o dell'Amministratore Delegato (laddove sia stata conferita apposita delega). Inoltre, tali Società Estere sono tenute a promuovere il recepimento del GCP verso le proprie controllate.

L'Organo Amministrativo di ciascuna Società Estera, in conformità alla propria autonomia e indipendenza:

- adotta le misure più appropriate per l'implementazione e il monitoraggio dell'attuazione del GCP, tenendo conto dell'organizzazione, della complessità delle attività, del profilo di rischio specifico e del quadro normativo applicabile alla società;
- è responsabile dell'adozione, implementazione e monitoraggio, laddove richiesto dalle normative nazionali, di propri Compliance Program Locali, richiamati anch'essi nell'Allegato Paese di riferimento;
- è responsabile della corretta individuazione di qualsiasi Processo, Area a Rischio o Principio di Comportamento, ulteriore rispetto a quanto individuato nell'ambito del GCP, da attuare attraverso Compliance Program Locali, linee guida, procedure, politiche interne locali ecc.

[4] In virtù della Delibera del 10 novembre 2017.
[5] In attuazione della facoltà di subdelega conferita all'Amministratore Delegato di Terna e tenuto conto di quanto previsto dalla LG001 "Il Sistema normativo Aziendale" le Appendici A a01LG058, B a02LG058 e C a03LG058 potranno essere aggiornate dal Direttore Strategia, Digitale e Sostenibilità di Terna S.p.A.
[6] In ogni caso, le società controllanti di diritto italiano sono dotate di un Compliance Program in linea con la normativa italiana, i.e. il Modello di Organizzazione, Gestione e Controllo ex Decreto Legislativo 231/2001 in linea con quanto previsto dalla LG032 del Gruppo Terna "Implementazione e gestione dei Modelli Organizzativi ex d.lgs. 231/2001 nel Gruppo Terna.

7. Risk Assessment

Alla base di ogni programma di compliance adottato da ciascuna Società Estere per l'attuazione del GCP deve svolgersi un'analisi dei processi aziendali volta a identificare e valutare i potenziali rischi di commissione delle fattispecie di Reati rilevanti ed i relativi presidi esistenti (cd. "**Risk Assessment**").

Le **fasi** che compongono il Risk Assessment sono le seguenti:

(i) **mappatura Aree a Rischio**, ossia individuare e mappare, nell'ambito dei singoli processi aziendali, le aree e le relative attività che sono potenzialmente esposte al rischio di commissione dei Reati;

(ii) **valutazione del grado di Rischio Potenziale**, effettuata alla luce dei possibili fattori idonei a generare il Rischio. Per **Rischio** si intende qualsiasi evento futuro che nell'ambito dell'azienda, da solo o in correlazione con altri eventi interni o esterni, può influenzare negativamente il raggiungimento degli obiettivi indicati nelle normative di riferimento del singolo Paese. La possibilità che un evento futuro e incerto in una specifica area/processo aziendale realizzi un Rischio costituisce un **Rischio Potenziale**;

(iii) **valutazione dell'adeguatezza dei protocolli interni**, al fine di individuare tutte le procedure e i controlli idonei a mitigare i rischi potenziali, nonché eventuali necessità di adeguare tali controlli. Il sistema di controlli preventivi deve essere tale da garantire che i Rischi di commissione dei Reati, secondo le modalità individuate e documentate nella fase precedente, siano ridotti ad un "livello accettabile";

(iv) **calcolo del rischio residuo (il "Rischio Residuo")**, inteso come il Rischio di Reati connesso a una specifica area/processo aziendale mitigato dall'esistenza ed effettività dei controlli interni adottati.

Tenendo in considerazione gli esiti del Risk Assessment e la strategia di Risk Management individuata per evitare, ridurre, accettare, monitorare e trasferire il rischio, deve essere effettuato un piano di interventi finalizzati al miglioramento del sistema di controllo (l'**Action plan**).

Il Risk Assessment in ambito GCP viene svolto da ogni SE (sulla base della metodologia individuata e messa a disposizione da Terna) su input della struttura CMP-PCR - di norma - su base annuale e comunque, ogni qual volta risulti necessario in virtù dell'aggiornamento del Global Compliance Program. Le Società Estere, per il tramite del proprio Compliance Officer, dovranno fornire evidenza alla struttura CMP-PCR dei risultati del Risk Assessment nonché degli eventuali Action Plan definiti a mitigazione dei rischi.

Il Risk Assessment dovrà considerare, preliminarmente, i Processi e le Aree di Rischio indicati nel GCP in relazione alla potenziale commissione dei Reati individuati al Par. 13.4.

Tale Risk Assessment, dunque, non esime le Società Estere (a) dall'effettuare la propria ulteriore valutazione del rischio di non conformità con riferimento alla normativa locale applicabile nonché alle peculiarità della propria attività e struttura organizzativa e (b) dal definire, laddove opportuno,

propri standard di controllo e Principi di Comportamento integrativi rispetto a quelli contenuti nel presente GCP.
Le singole Società Estere aggiornano costantemente la propria valutazione dei Rischi.

8. Compliance Governance

La governance per il presidio del GCP prevede le seguenti figure:
- Compliance Officer;
- Local Compliance Assistant;
- Struttura CMP-PCR di Terna.

8.1 Compliance Officer

In ciascuna Società Estera è nominato, con delibera dell'Organo Amministrativo, un **Compliance Officer** (o "**CO**").
Il CO deve essere in possesso di:

- competenze adeguate in materia giuridica o di controllo e gestione dei rischi aziendali, da valutare alla luce del curriculum vitae e delle esperienze professionali pregresse;
- requisiti di onorabilità, da valutare tenendo conto della condotta pregressa e del rispetto dei principi etici che governano l'operato del Gruppo Terna.

Il CO ha il compito di garantire la conformità della SE al GCP, di favorirne la diffusione e la conoscenza nonché agevolarne il funzionamento attraverso le attività di formazione/informazione e attraverso i flussi informativi di cui all'Appendice B (a02LG058).

Il Compliance Officer è inoltre responsabile di garantire la conformità alle singole normative applicabili in materia di Corporate Liability nei Paesi in cui opera la Società Estere tramite l'adozione di eventuali Compliance Program locali.

Il CO deve:
- favorire la diffusione e la conoscenza del Global Compliance Program e dei Compliance Program Locali adottati come previsti nell'Allegato Paese di riferimento e degli indirizzi della Capogruppo attraverso le attività di formazione necessarie;
- monitorare i comportamenti posti in essere all'interno della SE ed effettuare i controlli per l'accertamento di presunte violazioni delle prescrizioni del Global Compliance Program come integrato dal relativo Allegato Paese;
- coordinarsi con il Management Locale della SE per il monitoraggio delle attività nelle Aree a Rischio;
- monitorare l'effettiva attuazione di tutte le necessarie misure disciplinari emesse dalle strutture competenti della SE al fine di punire qualsiasi colpevole discostamento dalle regole di comportamento prestabilite;

- informare periodicamente l'Organo Amministrativo della Società Estera, relativamente ad ogni rilevante iniziativa intrapresa riguardante il Global Compliance Program e i Compliance Program Locali adottati nelle specifiche società indicate nell'Allegato Paese;
- informare tempestivamente l'Organo Amministrativo della Società Estera e la struttura CMP-PCR relativamente ad ogni eventuale accertata violazione (i) del Global Compliance Program; (ii) dell'Allegato Paese di riferimento, ivi compresi i Compliance Program Locali quali specifici presidi locali adottati (iii) delle procedure e delle Linee Guida valevoli per il Gruppo Terna nonché (iv) delle relative sanzioni disciplinari adottate;
- svolgere i compiti richiamati nel paragrafo dedicato in materia di Whisteblowing.

Ai fini del corretto svolgimento di tali attività, al CO viene garantita un'adeguata autonomia e indipendenza, anche rispetto al Management Locale. Il CO deve essere dotato di effettivi poteri di ispezione e controllo, nonché avere possibilità di accesso alle informazioni aziendali rilevanti.

In ogni caso, la Società Estera mette a disposizione del proprio CO ogni risorsa che dovesse rendersi necessaria o opportuna per l'efficace espletamento delle funzioni di vigilanza, compreso il supporto di eventuali professionisti esterni individuati dal CO medesimo per valutazioni tecniche di particolare complessità. Per tali ragioni la Società Estera attribuisce al CO risorse finanziarie e personali sufficienti per lo svolgimento della propria attività atti a garantire l'efficace implementazione del GCP e dei Compliance Program locali.

Il CO è deputato ad informare periodicamente la struttura CMP-PCR di Terna attraverso gli appositi flussi informativi individuati nell'Appendice B (a02LG058) del GCP. Tale individuazione potrà essere ulteriormente dettagliata nell'ambito di ciascun Allegato Paese, in ragione delle peculiarità organizzative e dell'attività della società stessa.

8.2 Local Compliance Assistant

Per le Società Estere che siano a loro volta delle subholding[7] del Gruppo Terna, il CO per l'esecuzione dei propri compiti, è eventualmente affiancato dal Local Assistant nominato con delibera dell'Organo Amministrativo della SE e previo parere positivo dello stesso CO.
Tale soggetto può essere individuato all'interno di una funzione aziendale della stessa SE in cui sia già stato nominato un CO.

Il Local Compliance Assistant ha il compito di supportare il CO nelle attività di:
- attuazione del GCP e della normativa locale in materia di Corporate liability nell'ambito della SE;
- gestione dei flussi informativi riguardanti la Società Estera;
- monitoraggio a livello locale dei corsi di formazione;
- gestione delle attività di informazione;

[7] Alla data di approvazione del GCP si intendono Subholding del Gruppo Terna: (i) la società Brugg Cable Service AG, società di diritto svizzero operante nel settore dei cavi che a sua volta, per il tramite delle proprie società controllate e Business Unit, opera nei seguenti Paesi: Svizzera; Germania; Cina; USA; India; Emirati Arabi; Arabia Saudita; (ii) la società Tamini Trasformatori S.r.l, società italiana attiva nella produzione di trasformatori che a sua volta controlla le società Tamini Transformers USA LLC e Tamini Trasformatori India Private Limited.

- elaborazione del Risk Assessment relativo alla singola SE;
- ogni altra attività che si dovesse rendere necessaria a supporto del CO.

8.3 Struttura CMP-PCR

La struttura CMP-PCR cura l'aggiornamento del Global Compliance Program; verifica e monitora l'attuazione degli Standard generali di controllo e dei Principi di Comportamento definiti per limitare il rischio di commissione dei Reati; diffonde la conoscenza del GCP e ne agevola il funzionamento attraverso:

- le attività di formazione/informazione ai CO e agli Amministratori delle SE come meglio dettagliato al par.9;
- la pianificazione e l'informativa all'Organo Amministrativo della Società Estera relativamente alle attività di monitoraggio e verifiche sul GCP e agli esiti delle verifiche stesse;
- l'informativa periodica, almeno su base annuale, all'Organismo di Vigilanza di Terna S.p.A in qualità di Capogruppo e gli Organismi di Vigilanza delle Società italiane che direttamente o indirettamente controllano la SE relativamente ad ogni iniziativa intrapresa riguardante il Global Compliance Program;
- l'implementazione di appositi flussi informativi da e verso le Società Estere per il tramite dei CO. Tali flussi, indicati nell'Appendice B (a02LG058) devono pervenire alla struttura CMP-PCR con cadenza periodica con l'obiettivo di monitorare il corretto funzionamento del GCP presso le Società Estere del Gruppo;
- il monitoraggio sull'efficace attuazione del GCP.

La struttura CMP-PCR organizza uno o più specifici incontri annuali con i Compliance Officers delle SE per garantire il coordinamento nella gestione delle tematiche di compliance del GCP.

9. Formazione e informazione

Terna S.p.A. promuove la conoscenza e la diffusione dei contenuti del Global Compliance Program. La struttura CMP-PCR, per il tramite della struttura Risorse Umane di TERNA organizza periodicamente sessioni di formazione obbligatorie per tutti gli Amministratori delle Società Estere nonché i CO sul Global Compliance Program.

Per l'ulteriore divulgazione dei contenuti del GCP agli altri Esponenti Aziendali, la struttura CMP-PCR ha il compito di aggiornare il materiale a supporto della formazione sul GCP ad essi destinata e di trasmetterlo ai CO affinché questi ultimi diffondano a loro volta la formazione a tutta la popolazione aziendale della SE.

Le attività di informazione e di formazione devono essere documentate, monitorate e valutate in termini di adeguatezza ed efficacia.

Pertanto, ciascuna Società Estera monitora le attività di formazione sui contenuti del GCP - e degli ulteriori Compliance Program eventualmente previsti per far fronte agli specifici rischi individuati localmente - e monitora che il percorso formativo pianificato venga fruito da tutto il personale interessato. In tal modo, gli Esponenti Aziendali saranno messi nelle condizioni di comprendere chiaramente ed essere consapevoli dei diversi Reati, dei rischi, delle relative responsabilità personali e aziendali e delle azioni da realizzare per prevenire la commissione di attività illecite.

Ogni Società Estera è dunque responsabile nel garantire un adeguato livello di partecipazione alla formazione per gli Esponenti Aziendali e di informazione per i Destinatari sul Global Compliance Program e sui propri Compliance Program Locali e procedure locali.

La SE garantisce che la documentazione aziendale in materia di etica e compliance, incluso il GCP, sia resa disponibile agli Esponenti Aziendali mediante pubblicazione sulla rete intranet aziendale o portali della Capogruppo o mediante invio via mail o altre modalità di condivisione di documenti aziendali e che ad ogni neoassunto sia consegnata (o indicata e messa a disposizione con le modalità sopra individuate) la documentazione in materia di compliance di riferimento per la SE.

Al personale neoassunto verrà fatta firmare apposita dichiarazione di presa visione e di impegno al rispetto dei principi contenuti nella documentazione relativa all'etica e alla compliance.

I principi e i contenuti del GCP che siano applicabili ai Terzi, sono resi conoscibili attraverso la documentazione contrattuale che dovrà prevedere clausole volte a garantire il rispetto da parte del Terzo dei Principi di Comportamento individuati dal GCP a loro direttamente applicabili. Laddove la SE abbia adottato un proprio Compliance Program Locale, le clausole contrattuali dovranno altresì prevedere il rispetto dei predetti programmi e delle normative applicabili.

10. Sistema di Whistleblowing

10.1 Sistema di reporting (Whistleblowing)

Chiunque può segnalare atti e/o comportamenti illeciti, commissivi o omissivi che costituiscono violazioni - anche sospette - dei Principi di Comportamento di cui al GCP e dei Compliance Program Locali dei principi sanciti nel Codice Etico, della normativa interna, rappresentata da tutte le disposizioni, procedure, linee guida o istruzioni operative della società destinataria della segnalazione nonché violazioni di policy, regole aziendali che possano tradursi in fattispecie di reato o, in ogni caso, che possano comportare un danno per il Gruppo o per le singole società del Gruppo.

Gli Esponenti Aziendali hanno il dovere di segnalare ogni violazione o presunta violazione del Codice Etico, dei Principi di Comportamento di cui al GCP e dei Compliance Program Locali adottati nella specifica SE indicati nel relativo Allegato Paese.

Le segnalazioni attinenti a violazioni accertate del GCP e dei Compliance Program Locali e dei loro atti attuativi adottati nella specifica SE riportati nell'Allegato Paese di riferimento, devono essere sempre portate a conoscenza del CO.
Inoltre, il CO viene tempestivamente informato circa l'esito dell'istruttorie sulle segnalazioni comunque attinenti a violazioni del GCP e dei Compliance Program locali, così da poter monitorare le azioni di miglioramento dei presidi di controllo.

Le Società Estere devono istituire un sistema di segnalazione delle violazioni tenendo conto della normativa locale in materia di segnalazioni whistleblowing (ove esistente e applicabile) e indicarne il gestore, spiegare il sistema di segnalazione delle violazioni, garantire la riservatezza dell'identità del segnalante e la confidenzialità sui contenuti della segnalazione, fatti salvi gli obblighi di Legge, tutelare chi effettui segnalazioni in buona fede e con uno spirito di lealtà nei confronti dell'azienda da ritorsioni o effetti negativi sulla sua posizione professionale; raccogliere le segnalazioni, valutarle secondo le procedure previste e definire le eventuali, in caso di accertata violazione, sanzioni commisurate alla gravità della violazione.

La disciplina di whistleblowing declinata nel Global Compliance Program prevede canali di segnalazione e tutele per il segnalante ed il segnalato e si applica anche alle Società Estere nel rispetto della legislazione locale.
Al riguardo la modalità di segnalazione e la gestione delle segnalazioni Whistleblowing sono disciplinate nella LG054, e sono applicabili anche alle Società Estere che abbiano aderito, nel rispetto della legislazione locale, al sistema di gestione predisposto da TERNA descritto nella stessa LG054 e adeguatamente regolato tramite accordi infragruppo tale attività e il trattamento dei dati in conformità alla legge applicabile.

Invece, in caso di impossibilità della SE di adottare la disciplina del whistleblowing con i canali di segnalazione interni così come descritti nella LG054, le SE appresteranno modalità di segnalazione delle informazioni sulle violazioni, nonché idonei flussi informativi verso il CO e TERNA riguardo ai presidi istituiti o da istituire e alle segnalazioni come di seguito descritto.

a) Whistleblowing secondo LG054

Nel caso in cui a seguito di attenta valutazione della normativa applicabile la SE aderisca al sistema di segnalazione previsto nella LG054 i canali interni di segnalazione previsti sono:
1. **Portale informatico**, accessibile al seguente indirizzo:
https://whistleblowing.terna.it/Segnalazioni/InvioSegnalazione (ITA/ENG).
2. **Posta ordinaria all'indirizzo**: Responsabile Audit c/o TERNA S.p.A., Viale Egidio Galbani, 70 – 00156 Roma, utilizzando la seguente dicitura "segnalazione whistleblowing, riservata – non aprire".
3. **Incontro diretto**: il segnalante ha la possibilità di richiedere un incontro con il Responsabile Audit al fine di comunicargli direttamente l'oggetto della segnalazione. Suddetto incontro viene fissato tramite una richiesta effettuata dal segnalante tramite Portale (https://whistleblowing.terna.it/Segnalazioni/InvioSegnalazione) o apposita e-mail all'indirizzo whistleblowing@terna.it, specificando il nome della società del Gruppo Terna oggetto della segnalazione.

Le disposizioni della LG054 applicabili saranno quelle previste per le segnalazioni ordinarie, ovvero le segnalazioni non rientranti nell'ambito di applicabilità del D.lgs. 24/2023[8], non essendo applicabile la specifica normativa italiana in materia.

Deve essere garantito il trattamento dei dati personali secondo la disciplina in materia applicabile, nonché il generale divieto di ritorsioni previsto dal Codice Etico, espressamente sanzionabile per le segnalazioni effettuate in buona fede e con uno spirito di lealtà nei confronti dell'azienda.

Per quanto attiene ai ruoli e alle responsabilità, nel trattamento delle segnalazioni che resta in capo al Gestore, può essere richiesto supporto al Compliance Officer nominato dalla società interessata e/o di consulenti esterni; il coinvolgimento del CO in tale fase è circoscritto all'acquisizione di informazioni funzionali all'istruttoria.

Ad esito dell'istruttoria, il Gestore dà informativa al CO delle violazioni accertate del GCP e dei Compliance Program Locali e/o delle azioni di miglioramento necessarie a rafforzare i presidi di controllo interni.

b) Whistleblowing Società Estere

In caso di impossibilità della SE di aderire alle modalità di gestione delle segnalazioni Whistleblowing definite nell'ambito della LG054, le SE apprestano, in linea con la normativa locale, modalità di segnalazione delle informazioni sulle violazioni coerenti con le tutele del segnalante previste dal Codice Etico e provvedono a:

- comunicare a Terna S.p.A., anche tramite il CO, i presidi istituiti o da istituire che possono prevedere il coinvolgimento del CO nominato ai sensi del Global Compliance Program;
- assicurare adeguata informazione circa il sistema di segnalazione delle informazioni sulle violazioni, le modalità di utilizzo e il sistema di tutele approntato.

La SE, inoltre, dovrà implementare un adeguato sistema di monitoraggio propedeutico alla definizione di una reportistica annuale verso Terna S.p.A., anche per il tramite del CO, relativa alle segnalazioni ricevute, con l'indicazione delle seguenti informazioni:

- numero di segnalazioni pervenute;
- numero di segnalazioni esaminate;
- breve descrizione dell'area normativa della segnalazione (ad es. Privacy; Cyber security; Corporate governance; Salute e sicurezza; Risorse Umane; Sostenibilità; Fiscale; Acquisti; Security), con specifica evidenza (anche ai fini dell'attività di rendicontazione di sostenibilità) del numero di casi in cui sono state segnalate discriminazioni o molestie;
- numero di segnalazioni archiviate "senza fondamento";
- numero di segnalazioni fondate "con seguito e con provvedimento; rispetto alle quali dovrà essere indicata la tipologia delle attività promosse;
- numero di segnalazioni fondate "con seguito senza provvedimento", rispetto alle quali dovrà essere indicata la tipologia delle attività promosse.

[8] Cfr. LG054 Whistleblowing, pag. 6 par. 2

In nessuno caso dovrà essere condiviso con Terna S.p.A. l'oggetto e/o contenuto delle segnalazioni ricevute.
Tale reportistica sarà rivolta, oltre che verso il proprio AD/AU/Executive Director e il proprio CO, anche verso il Chief Risk Officer, il Responsabile Internal Audit e il Comitato Etico nominati da Terna.

La SE dovrà inoltre individuare il gestore del canale di segnalazione apprestato nel rispetto della disciplina sul trattamento dei dati personali applicabile e chi analizza e promuove le azioni più opportune in base alle risultanze istruttorie nonché declinare i presidi di gestione con propria disposizione/procedura aggiornando altresì i richiami nei Compliance Program locali e sul sito internet ove disponibile.

10.2 Investigation

Tutte le volte in cui è ricevuta una segnalazione, si attiva un processo volto a gestire la segnalazione e a monitorare la sua tempestiva risoluzione. Tale processo è attuato e tracciato a cura dei soggetti formalmente individuati per la gestione delle segnalazioni.
A seguito della segnalazione, gli Esponenti Aziendali sono tenuti a cooperare con le relative indagini ove coinvolti nell'istruttoria.
La mancata cooperazione e la mancata trasmissione di informazioni oneste e veritiere potrebbero determinare l'adozione di azioni disciplinari.
Sulla base delle risultanze verranno adottate le azioni più opportune nei confronti del segnalante, del soggetto segnalato, nonché le azioni correttive più adeguate con riferimento ai Processi interessati dalla segnalazione.

11. Monitoraggio e miglioramento continuo

La struttura CMP-PCR monitora sull'efficace attuazione del GCP.
In particolare, è previsto lo svolgimento di periodiche attività di audit e di testing volte a:

- assicurare l'efficacia del GCP;
- intercettare eventuali violazioni;
- individuare eventuali azioni di miglioramento o correttive a livello organizzativo o nell'ambito dei singoli Processi, in ottica di rafforzare il Sistema di Controllo Interno e Gestione dei Rischi.

Inoltre, il monitoraggio sull'effettiva attuazione locale del GCP, così come integrato dal relativo Allegato Paese da parte da parte delle Società Estere, viene effettuato dal CO.

In caso di dubbi sull'interpretazione, sull'implementazione e sull'applicabilità di qualsiasi Area a Rischio, degli Standard Generali di Controllo o dei Principi di Comportamento, ciascun Esponente Aziendale dovrà consultarsi preliminarmente, per il tramite del proprio CO, con la struttura CMP-PCR.

12. Sistema sanzionatorio

Le violazioni delle leggi sulla responsabilità penale o assimilabile delle persone giuridiche possono avere conseguenze penali, civili e amministrative, tra cui l'irrogazione di sanzioni (pecuniarie e interdittive) e la reclusione, così come un grave danno alla reputazione del Gruppo Terna.

La piena effettività del GCP e/o di una politica, una procedura o un'istruzione locale a esso correlata o di qualsiasi altra procedura del Gruppo Terna applicabile, nonché dei Compliance Program Locali, viene garantita mediante l'applicazione di apposite sanzioni in caso di violazione dei principi contenuti nei predetti documenti.

In caso di violazioni commesse dagli Esponenti Aziendali, le relative sanzioni disciplinari saranno comminate dalla singola Società Estera, in conformità con la regolamentazione locale applicabile in materia, nonché sulla base dei Compliance Program Locali.

In aggiunta, le Società Estere adotteranno adeguate sanzioni in caso di (i) violazione delle normative locali in materia di *corporate liability* (laddove applicabili); (ii) atti di ritorsione o discriminatori, diretti o indiretti, nei confronti di eventuali whistleblower per motivi collegati alla segnalazione (iii) violazione delle misure di tutela del whistleblower e di effettuazione con dolo o colpa grave di segnalazioni che si rivelino infondate.

Tra le sanzioni applicabili possono essere previste quella della cessazione del rapporto di lavoro e del risarcimento dei danni.
Le sanzioni dovranno essere applicate a prescindere dagli esiti di eventuali procedimenti penali avviati dalle autorità giudiziarie competenti.

In caso di violazioni da parte dei Terzi, ciascuna Società Estera adotterà appropriate misure, compresa – a titolo esemplificativo ma non esaustivo – la risoluzione del contratto.

13. Il GCP e gli standard generali di controllo

13.1 Il GCP e i riferimenti di controllo TERNA

I dettami del GCP sono in generale ispirati all'insieme della cultura, delle capacità, delle regole, delle procedure e delle pratiche aziendali, nonché delle strutture organizzative, volti a definire un sistema di accountability per l'identificazione, misurazione, gestione, mitigazione e controllo dei principali rischi a livello di Gruppo mantenendo di conseguenza alta la fiducia degli stakeholders con riguardo al governo e al controllo del Gruppo medesimo, nel complesso, definito come il "Sistema di Controllo Interno e di Gestione dei Rischi" o "SCIGR".

I Principi di Comportamento definiti all'interno del GCP sono integrati dagli indirizzi stabiliti dalle Politiche, Linee Guida, Istruzioni Operative e dal resto delle procedure della Capogruppo così come applicabili nelle Società Estere.

Al fine di assicurare l'efficacia del SCIGR in ambito GCP sono considerati i documenti richiamati nell' Appendice C (a03LG058).

La struttura Affari Societari Controllate (di seguito **AGLS-ASCO**), direttamente o indirettamente, garantisce la diffusione presso le Società Estere – nonché il conseguente formale recepimento da parte delle stesse - della normativa che costituisce parte integrante del Sistema di Controllo Interno. Pertanto, in seguito alla pubblicazione di una nuova Politica, Linea Guida, Istruzione Operativa o altro documento riconducibile al GCP, oppure in caso di aggiornamento di tale normativa già esistente, la struttura AGLS-ASCO – su input/informativa delle strutture competenti per il presidio del sistema documentale di Terna (HSEQ-DOC o di OHP-ORG) - avrà cura di inviare il documento alle Società Estere interessate in base all'ambito di applicazione definito dalla struttura owner del documento. (eventualmente, in caso di subholding dando mandato a procedere per la capillare diffusione verso tutte le Società Estere da queste controllate). A tal fine l'owner del documento individuato all'interno delle Linee Guida e delle Istruzioni Operative disciplina l'ambito di applicazione dello stesso e ne assicura la traduzione, così come previsto dalla normativa sul sistema documentale di Terna.

Qualora la struttura AGLS-ASCO richieda chiarimenti al riguardo o maggiore dettagli rispetto a quanto indicato dall'owner sarà cura della struttura HSEQ-DOC o OHP-ORG chiedere informazioni supplementari alla struttura owner e, comunicarle alla struttura AGLS-ASCO.

Nell'invio del documento alle Società Estere dovrà essere tenuta in copia la struttura CMP-PCR nonché la struttura owner del documento.
Laddove, a seguito di attenta valutazione, sussista necessità di deroga e/o di parziale inapplicabilità di tale normativa, o laddove fossero necessari eventuali chiarimenti, la Società Estera, anche per il tramite del proprio Compliance Officer, dovrà condividere tali valutazioni con la struttura owner del documento avvalendosi - eventualmente - anche del supporto delle strutture ASC-ASC e CMP-PCR. Le deroghe, che devono avere carattere eccezionale, vanno adeguatamente motivate e circostanziate.

Le Società Estere sono tenute a conservare evidenza delle valutazioni che giustifichino l'eventuale non applicabilità dei dettami del GCP e della normativa parte del SCIGR, qualora in contrasto con la normativa locale.

Le evidenze del recepimento del Sistema di Controllo Interno da parte della Società Estera dovranno confluire nell'Allegato Paese di riferimento.

La struttura CMP-PCR effettuerà, con cadenza almeno annuale, un'attività di verifica dello stato di recepimento e applicazione del Sistema di Controllo Interno da parte delle Società Estere, coordinandosi con AGLS-ASCO e predisponendo eventuali azioni correttive. Tale attività rientra nel più ampio framework di controllo volto a garantire l'allineamento delle Società Estere agli standard aziendali e normativi applicabili.

Ogni volta che viene costituita una nuova Società Estera, oppure quando una Società Estera già esistente è interessata da modifiche strutturali e organizzative (ad esempio operazioni straordinarie come fusioni, acquisizioni o vendita di un ramo d'azienda), la Società Estera provvederà ad istituire il proprio Sistema di Controllo interno coerentemente con quanto stabilito nell'ambito del Global Compliance Program. Per tali finalità la struttura AGLS-ASCO provvederà a diffondere alle Società Estere gli atti di indirizzo che costituiscono parte integrante del SCIGR informando contestualmente anche CMP-PCR.

Oltre a quanto sopra descritto, ciascuna Società Estera integrerà le previsioni del GCP con regole previste nello specifico Allegato Paese adottato da ciascuna SE includendo anche:

i. i Compliance Program Locali;
ii. le disposizioni di corporate governance adottate dalle stesse SE in conformità alla legislazione applicabile e alle best practice internazionali;
iii. il sistema di controllo interno e di gestione dei rischi adottato in ciascuna Società Estera (e.g. procedure e policy locali, principi di comportamento, ecc.).

Qualora leggi o normative locali o politiche e procedure aziendali così adottate dalle singole Società Estere prevedano regole più stringenti rispetto a quelle contenute nel presente GCP, le prime prevarranno.

13.2 Standard Generali di Controllo

Ogni Società Estera nel valutare l'opportunità di dotarsi di procedure locali – tenendo in considerazione la peculiare attività svolta e i relativi rischi associati individuati in base al Risk Assessment di cui al paragrafo 7 – dovrà in ogni caso:

- prevedere gli Standard Generali di Controllo individuati di seguito;
- dettagliare i controlli interni;
- prevedere l'applicazione di sanzioni disciplinari in caso di violazione delle stesse procedure;
- prevedere processi decisionali basati su criteri oggettivi e imparziali.

A tal fine ogni qual volta un Esponente Aziendale, si trovi in una situazione di conflitto (potenziale o accertato) tra l'interesse personale e quello dell'azienda deve darne comunicazione al fine della corretta gestione del conflitto.

Gli Standard Generali di Controllo sono i seguenti:

- **segregazione dei ruoli**: l'assegnazione di ruoli, compiti e responsabilità all'interno di ogni società deve essere effettuata in conformità al principio di segregazione dei ruoli secondo cui nessun individuo può svolgere autonomamente un intero processo (i.e. secondo questo principio, nessun individuo può, da solo e in autonomia, eseguire un'azione, autorizzarla e successivamente controllarne l'esecuzione). Un'adeguata segregazione dei ruoli può essere garantita anche utilizzando sistemi informatici che consentano solo alle persone identificate e autorizzate di svolgere determinate operazioni;

- **potere di firma e autorizzazione**: ciascuna società deve emanare disposizioni formali in relazione all'esercizio dei poteri autorizzativi e di firma che devono essere coerenti con le responsabilità organizzative e gestionali attribuite;
- **trasparenza e tracciabilità dei processi**: l'identificazione e la tracciabilità delle fonti, delle informazioni e dei controlli effettuati in relazione alla formazione e all'attuazione delle decisioni della Società Estera, nonché in relazione alla gestione delle risorse finanziarie, deve sempre essere garantita; è altresì opportuno garantire la corretta registrazione dei relativi dati e delle informazioni, attraverso sistemi informatici e/o supporto cartaceo;
- **corretta gestione delle relazioni con i Terzi e Due Diligence** (si veda par. 13.3).

13.3 Standard di gestione delle relazioni con i Terzi e Due Diligence

TERNA e le società del Gruppo Terna prestano particolare attenzione alla selezione dei Terzi. A tal fine, ogni volta che una società è impegnata in attività di business oppure intende rivolgersi a un Terzo in connessione a qualsiasi business da parte delle strutture competenti, deve essere condotta un'indagine sul Terzo, volta a individuarne la catena di controllo, il possesso di requisiti di onorabilità, professionali e finanziari, la sua credibilità sul mercato, nonché la sua conformità alle Leggi Anti-Corruzione vigenti, o leggi simili previste dal Paese in cui opera o opererà anche per conto di qualsiasi società del Gruppo Terna.

La Due Diligence dovrà essere proporzionata al rischio reale o percepito in relazione al Terzo e/o all'operazione (risk based).
La Due Diligence è condotta, sulla base dei criteri individuati dalla Capogruppo, che potranno includere tra gli altri: (i) ricerche tramite fonti pubbliche e altre fonti disponibili (ad es. contatti di business, camere di commercio locali, associazioni di imprese; ricerche su web o società specializzate, iscrizioni in Liste) su società, soci ed esponenti, al fine di reperire eventuali informazioni negative potenzialmente rilevanti a carico degli stessi; (ii) o approfondimenti svolti da consulenti terzi.

La Due Diligence è disciplinata da linee guida di indirizzo per il Gruppo di cui all'Appendice – (a03LG058), nonché dalle procedure locali adottate dalle SE, ove esistenti.

In ogni caso, la Due Diligence condotta dovrà evidenziare potenziali Red Flag.

Di seguito sono elencati alcuni esempi di Red Flag che possono essere presi in considerazione nell'esecuzione della Due Diligence, quali potenziali fattori di rischio o indicatori della possibile commissione di Reati:
- la potenziale Controparte non è solida dal punto di vista economico - finanziario o presenta situazioni economico - finanziarie negative;
- la potenziale Controparte è indagata / imputata o condannata per uno o più reati;
- se il Terzo o, in caso di società, i suoi soci, sono residenti o hanno sede legale o svolgono la propria attività in un Paese presente nelle cd. "black list"/"grey list" internazionali antiriciclaggio (ad es. pubblicate dal GAFI e dall'Unione Europea) o in un Paese identificato come Paese che

fornisce supporto ad attività terroristiche o nel cui territorio operano organizzazioni terroristiche ovvero in quei Paesi considerati quali "Paradisi Fiscali" così come individuati da organismi nazionali e/o internazionali riconosciuti (es. Agenzia delle Entrate, OCSE) o in un Paese ad alto rischio corruzione (si veda ad es. ranking di Transparency International) o sottoposti a sanzioni internazionali;

- difficoltà di identificare il beneficiario ultimo della potenziale Controparte a causa di elementi insufficienti, false o inconsistenti informazioni o a causa delle leggi del Paese in cui la Controparte ha la sede legale/residenza che non prevede obbligo di registrazione;
- se il Terzo svolge attività/business che non risultano coerenti o non conformi con la prestazione contrattuale richiesta o se il Terzo o uno dei suoi esponenti sia in conflitto di interessi;
- se vi siano comunque operazioni o richieste che non sono coerenti con l'attività svolta dal Terzo, quali richieste di pagamento presso un Paese ad alto rischio che non abbia alcuna connessione con il Terzo (per esempio, un Paese con leggi molto protettive in materia di segreto bancario, o con controlli deboli sul riciclaggio di denaro o dove la criminalità/la corruzione è diffusa). A tale scopo i Paesi ad alto rischio devono essere valutati tenendo conto di indici internazionali, come il Transparency International Corruption Perceptions Index;
- se vi sia la richiesta di strutturare un'operazione in maniera tale da eludere le normali regole di contabilità e reportistica o tale da non mostrare alcun legittimo scopo commerciale, per esempio aumentando i prezzi o effettuando una parte del pagamento "sotto traccia" attraverso la stesura di side letter;
- se occorra ricorrere a consulenti o ad altri Terzi che abbiano stretti legami con un governo o con un partito politico, o che siano stati specificamente segnalati da un Funzionario Pubblico o da un cliente;
- se vi siano richieste di pagamento di commissioni, provvigioni o altre forme di remunerazione inusuali o richieste di pagamenti in contanti;
- se il Terzo sia apparentemente privo delle competenze, esperienza o risorse richiesti per il tipo di attività oppure abbia una struttura organizzativa aziendale assente o mezzi patrimoniali non adeguati;
- se il Terzo, con riferimento all'operazione, rifiuti di sottoscrivere un contratto;
- se il Terzo rifiuti di impegnarsi a rispettare o di rispettare le presenti Linee Guida e/o ulteriori procedure interne di compliance adottate dalla SE e/o valevoli per il Gruppo e non abbia adottato alcun codice di condotta o strumento di compliance similare atto a prevenire la commissione di reati.

La presenza di una o più Red Flag richiede un esame maggiormente approfondito che può includere controlli addizionali e/o appropriati livelli autorizzativi.

In caso di transazioni ad alto rischio o per situazioni particolarmente complesse, le analisi possono essere integrate da pareri e approfondimenti su specifiche questioni affidati a provider o consulenti specializzati nelle materie di riferimento.

È necessario un monitoraggio nel corso del rapporto contrattuale per assicurare che il Terzo mantenga i requisiti individuati e approvati, se necessario aggiornando periodicamente la Due

Diligence. Nel caso in cui un Terzo perda tali requisiti o emerga un Red Flag durante la vigenza del rapporto contrattuale, dovranno essere definite misure appropriate da applicare.

I Terzi dovranno essere adeguatamente informati sui contenuti del GCP e, laddove esistenti, dei Compliance Program Locali e dovranno impegnarsi a rispettare i Principi di Comportamento contenuti nei predetti documenti mediante la sottoscrizione di apposite clausole contrattuali.

13.4 I reati da prevenire

Gli standard generali di controllo e Principi di Comportamento, associati ad ogni processo e relativa area a rischio di cui ai paragrafi 11 e ss, sono riferibili ai seguenti Reati:

A. Reati di Corruzione;
B. Altri reati verso la Pubblica Amministrazione;
C. Frodi contabili;
D. Reati tributari;
E. Market Abuse;
F. Reati di criminalità organizzata;
G. Riciclaggio e finanziamento del terrorismo;
H. Delitti contro la personalità individuale;
I. Reati in materia di Salute e sicurezza;
J. Reati ambientali;
K. Reati informatici.

L'Appendice A (a01LG058) descrive, a titolo meramente esemplificativo, le principali tipologie di comportamenti potenzialmente qualificabili come Reati nelle diverse giurisdizioni in cui il Gruppo Terna si trova ad operare.

14. Relazioni con enti pubblici e funzionari pubblici

I Principi di Comportamento di cui al presente paragrafo, relativi alle relazioni con gli enti pubblici e funzionari pubblici, costituiscono uno dei principali pilastri richiamati dal DOJ, data la rilevanza nel contesto internazionale della corruzione dei pubblici ufficiali, caposaldo delle principali normative (quali FCPA e UK Bribery Act).

Tali Principi di Comportamento devono intendersi applicabili in tutti i rapporti con detti soggetti e trasversalmente anche a tutti gli altri Processi disciplinati nel GCP.

Per ente pubblico o "Pubblica Amministrazione" ("P.A." o "ente pubblico") si intende ciascuno degli enti o apparati che concorrono all'esercizio delle funzioni legislativa, amministrativa o giudiziaria di un singolo stato, ivi compresi gli enti governativi.

Per funzionario pubblico ("**Funzionario Pubblico**") si intende, ai fini del presente documento, (a) qualunque funzionario, eletto o nominato che esercita una pubblica funzione legislativa, amministrativa o giudiziaria (b) qualunque persona che svolge funzioni pubbliche in qualsiasi ramo del governo nazionale, regionale o comunale o che esercita una funzione pubblica per qualsiasi agenzia o impresa pubblica, come i funzionari che esercitano funzioni pubbliche in imprese statali.

Per ciascuna Società Estera, le definizioni che precedono devono essere utilizzate tenendo conto della legislazione locale applicabile, così come i Reati astrattamente configurabili.

POSSIBILI AREE A RISCHIO

(i) Negoziazione e gestione dei contratti conclusi con Pubbliche Amministrazioni ed enti pubblici
(ii) Partecipazione a gare pubbliche;
(iii) Gestione delle relazioni - diverse dalle relazioni contrattuali - con enti pubblici;
(iv) Partecipazioni a ispezioni, indagini, accessi e verifiche espletate da Funzionari Pubblici;
(v) Gestione di finanziamenti pubblici ricevuti e sovvenzioni o garanzie ottenute;
(vi) Gestione delle controversie (processi, arbitrati, procedimenti extragiudiziali);
(vii) Selezione di partner, intermediari e consulenti nonché negoziazione e gestione dei relativi contratti;
(viii) Gestione dei flussi finanziari;
(ix) Invio di flussi informatici verso le Pubbliche Amministrazioni;
(x) Gestione delle iniziative no profit, corporate giving (incluse liberalità e sponsorizzazioni);
(xi) Gestione degli omaggi e delle spese di intrattenimento e di ospitalità;
(xii) Selezione e assunzione del personale;
(xiii) Rimborso spese sostenute dai dipendenti;
(xiv) Definizione dei criteri di incentivazione del management della SE.

PRINCIPI DI COMPORTAMENTO

Nella conduzione di qualsiasi attività che implichi un'interazione con Pubbliche Amministrazioni e/o Funzionari Pubblici, i Destinatari devono agire con integrità e onestà rispettando tutte le leggi e i regolamenti applicabili.

Per l'individuazione degli obblighi posti in capo ai Destinatari (in base a specifici accordi contrattuali) al fine di prevenire la commissione di reati di tipo corruttivo si fa rinvio alla LG059 "Anticorruzione".

Ai Destinatari e alle Terze Parti (in base a specifiche condizioni contrattuali), è **fatto divieto di**:

- effettuare elargizioni in denaro o di altra natura, di propria iniziativa o a seguito di sollecitazione, nei confronti di Pubblici Ufficiali e/o Esponenti della Pubblica Amministrazione, al fine di ottenere un'utilità per la società o per un terzo;
- offrire doni o spese di intrattenimento al di fuori di quanto ammesso dalla prassi della normativa locale e dalle regole di cui alla LG024 "Corporate Giving e Membership";
- utilizzare il contante come mezzo di pagamento al di fuori dei casi consentiti dalla normativa (ad esempio, la piccola cassa);
- presentare documentazione che contenga dati, informazioni non veritiere e/o ometta dati, informazioni, al fine di agevolare l'ottenimento di autorizzazioni/titoli in favore della società;
- sostenere spese promozionali o di sponsorizzazione al di fuori di quanto ammesso dalla LG024"Corporate Giving e Membership", e dalle ulteriori normative di Terna così come mappate nell'ambito dell'Appendice C (a03LG058).

Le Società Estere **dovranno garantire**:

- la **tracciabilità di qualsiasi relazione**, comunicazione e rapporto rilevante con la Pubblica Amministrazione (ad esempio procedimenti amministrativi volti ad ottenere un'autorizzazione, una licenza o atto simile, joint venture con enti pubblici, ecc.);
- il **coinvolgimento di almeno due soggetti** autorizzati nella gestione delle relazioni con la Pubblica Amministrazione;
- che le **assunzioni di personale** avvengano esclusivamente in base a necessità aziendali reali e dimostrabili, avvalendosi di un iter di selezione che coinvolga almeno due funzioni e che si basi su criteri di oggettività, competenza e professionalità, evitando qualsiasi favoritismo o conflitto di interessi o qualsiasi azione che si concretizzi in favoritismi, nepotismi o forme clientelari idonee ad influenzare l'indipendenza di un Funzionario Pubblico o ad indurlo ad assicurare un qualsiasi vantaggio per la Società Estera o per il Gruppo Terna;
- i **piani di incentivazione del management** sono adottati in modo tale che gli obiettivi prefissati non portino a comportamenti abusivi e siano, invece, focalizzati su un risultato possibile, determinato, misurabile e appropriato rispetto al tempo necessario per raggiungerli;
- la formalizzazione di eventuali accordi con i Funzionari Pubblici e P.A. (in forma scritta o contratti digitali);
- che tutte le **dichiarazioni rilasciate alle Pubbliche Amministrazioni** nazionali o internazionali (ad es. per ottenere fondi, sovvenzioni o prestiti) includano solo dati corretti e siano sottoscritte da soggetti autorizzati e che eventuali fondi, sovvenzioni o prestiti ottenuti siano adeguatamente contabilizzati;

- una **corretta separazione dei compiti**, assicurando che le fasi di richiesta, di gestione e di segnalazione in relazione ai procedimenti pubblici ai fini dell'ottenimento di fondi, sovvenzioni o prestiti pubblici siano gestiti da Esponenti Aziendali diversi all'interno dell'organizzazione;
- il **coinvolgimento** delle funzioni competenti nelle attività di raccolta e di analisi delle informazioni necessarie ai fini dell'espletamento di attività di rendicontazione;
- **l'approvazione** da parte di adeguati livelli gerarchici della documentazione e della successiva attività di rendicontazione da presentare in relazione alla richiesta di sovvenzioni, prestiti e garanzie.

Inoltre, i Destinatari, nell'ambito della relazione con le Pubbliche Amministrazioni, **non devono** in alcun modo:

a) inviare documenti falsi o artefatti, in tutto o in parte, durante la partecipazione a gare pubbliche;
b) indurre in qualsiasi forma la Pubblica Amministrazione ad effettuare una valutazione erronea durante l'esame di richieste di autorizzazione, licenze, nulla osta, concessioni, ecc.;
c) omettere informazioni dovute al fine di permettere ad una delle società del Gruppo Terna di ottenere un vantaggio a proprio favore in una qualsiasi delle circostanze di cui alle lettere a) e b) sopra indicate;
d) avere comportamenti finalizzati a ottenere da una Pubblica Amministrazione qualsiasi tipo di sovvenzione, finanziamento pubblico, prestito agevolato o altre erogazioni dello stesso tipo, mediante dichiarazioni e/o documenti artefatti o falsi o omissione di informazioni pertinenti o, più in generale, per mezzo di artificio o di inganno, volti a portare in errore l'istituzione;
e) utilizzare i fondi ricevuti da Pubbliche Amministrazioni per fini diversi da quelli per i quali sono stati concessi.

Inoltre, le SE presteranno particolare attenzione ai cd. **facilitation payments**, cioè ai pagamenti fatti allo scopo di accelerare o assicurare un'attività considerata di routine nell'esercizio di una funzione pubblica (per esempio, organizzazione di un'attività ispettiva, concessione di una licenza commerciale, formalità connesse ad operazioni di carico e scarico di merce) e ai contributi politici.

Pertanto, le SE **garantiscono**:

- che sia vietato ogni tipo di Facilitating Payments da parte degli Esponenti Aziendali e degli Altri Destinatari;
- che sia vietato ogni tipo di contributo politico a partiti o qualunque forma di sostegno a campagne politiche per conto della Società Estera o di una qualunque società del Gruppo Terna. Tali contributi politici o sostegni possono includere, ad esempio: a) denaro; b) beni diversi dal danaro (come, ad esempio attrezzature prestate o donate, servizi di tecnologia gratuiti, la messa a disposizione di risorse umane); e/o c) l'utilizzo di risorse societarie (come ad esempio: strutture, posta elettronica, uffici).

Tale regola non vieta comunque all'Esponente Aziendale di esercitare il suo diritto di partecipare ad attività politiche a livello inequivocabilmente personale.
Con riferimento ad eventuali altre Aree a Rischio non individuate nel presente paragrafo, si deve fare riferimento ai Principi di Comportamento individuati nei Processi indicati nel prosieguo e nella LG059 "Anticorruzione".

15. Comunicazione (Corporate Giving e Promotion)

I Principi di Comportamento di cui al presente paragrafo si riferiscono al processo di Comunicazione e più precisamente alle attività che impattano sulle attività di Corporate Giving e Promotion inclusa l'organizzazione di eventi.

POSSIBILI AREE DI RISCHIO

(i) Gestione delle attività di corporate giving (sponsorizzazioni e liberalità) e promotion (ad es. omaggi, spese di intrattenimento e ospitalità, ecc.);
(ii) Organizzazione di eventi.

PRINCIPI DI COMPORTAMENTO

Nell'ambito delle attività di "**Corporate Giving**" e "**promotion**", ai Destinatari è **fatto divieto** di distribuire e/o ricevere omaggi e regali o altri vantaggi di qualsiasi natura al di fuori di quanto previsto dalle policy aziendali richiamate nell'Appendice C (a03LG058).
A titolo esemplificativo e non esaustivo, è vietata qualsiasi attività di "promotion" - effettuata di propria iniziativa o a seguito di sollecitazione - intesa come omaggistica, ospitalità e spese di intrattenimento a Pubblici Ufficiali o Esponenti della Pubblica Amministrazione locali ed esteri (anche in quei Paesi in cui l'elargizione di doni rappresenta una prassi diffusa) nonché ai loro familiari, associazioni o enti nei cui organi direttivi tali soggetti siano presenti e che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per la Società.

I regali e le attività di intrattenimento ammessi includono, a titolo esemplificativo e non esaustivo: (i) pranzi, cene di modico valore e occasionali; (ii) doni di basso valore nominale come penne, calendari o altri oggetti promozionali.

I regali e le spese non ammessi includono, a titolo esemplificativo e non esaustivo: viaggi; regali o spese per eventi esterni di intrattenimento che coinvolgano soggetti con i quali la SE è attualmente impegnata o intende impegnarsi. Le regalie offerte così come quelle ricevute devono essere documentate in modo adeguato secondo quanto previsto dalle procedure aziendali richiamate all'Appendice C (a03LG058) e dalle ulteriori eventuali procedure locali della SE.

Le sponsorizzazioni e le liberalità debbono essere effettuate in coerenza con i principi e le metodologie definite nella relativa normativa applicabile per il Gruppo Terna.

Inoltre, le attività di corporate giving **devono**:
- essere effettuate coerentemente con i principi del Codice Etico e con le procedure aziendali applicabili in materia, e nei limiti del budget approvato;
- essere effettuate solo in favore di enti/soggetti affidabili e ben noti per integrità e correttezza professionale; a tal fine, gli Esponenti Aziendali devono svolgere verifiche preventive circa l'onorabilità dei soggetti beneficiari dell'attività di Corporate Giving;

- essere approvate secondo livelli autorizzativi adeguati e la relativa richiesta deve includere: (a) un'adeguata descrizione circa la natura e la finalità del singolo contributo/sponsorizzazione, (b) una Due Diligence sul beneficiario e (c) la verifica sulla legittimità del contributo o sponsorizzazione, in base alle leggi applicabili;
- essere formalizzate in appositi accordi scritti/lettere che (i) definiscano chiaramente l'oggetto e le finalità per le quali il contributo può essere utilizzato, (ii) prevedano, ove applicabili, controlli sull'utilizzo del contributo erogato in conformità a quanto previsto dall'accordo e (iii) contengano apposite previsioni volte a garantire il rispetto delle leggi applicabili.

Gli Esponenti Aziendali **sono tenuti** a:
- mantenere la tracciabilità dei processi autorizzativi dell'attività di corporate giving, garantendo la collegialità delle decisioni in merito;
- effettuare i pagamenti al beneficiario esclusivamente su un conto a questo intestato;
- verificare che i fondi versati siano stati utilizzati per gli scopi previsti;
- verificare ex post l'effettività della controprestazione nell'ambito delle attività di sponsorizzazione;
- informare con periodicità almeno annuale il CO e CMP-PCR delle attività di Corporate Giving, e promotion svolte nel corso del periodo di riferimento.

Con riferimento all'area "**Organizzazione di eventi**" è fatto obbligo per gli Esponenti aziendali di:
- assicurare che le finalità dell'evento e/o iniziative ad assimilabili siano chiaramente identificate, legittime e coerenti con gli indirizzi strategici e la brand identity del Gruppo;
- mantenere traccia dei processi autorizzativi dell'attività di organizzazione di eventi;
- garantire che tutti i costi siano giustificati, tracciati e coerenti con il budget pianificato e approvato;
- impegnarsi affinché l'organizzazione degli eventi aziendali dedicati agli organi di informazione sia regolata in modo tale da evitare l'offerta di doni o forme di intrattenimento che possano influenzare l'obiettività di giudizio e l'indipendenza degli organi di informazione partecipanti.

Inoltre, ai Destinatari è **fatto divieto di**:
- accordare vantaggi indebiti di qualsiasi natura;
- favorire terzi con cui si abbiano rapporti personali o che presentino situazioni di potenziale conflitto;
- acquisire o utilizzare prodotti tutelati da diritto d'autore in violazione delle tutele contrattuali previste per i diritti di proprietà intellettuale altrui.

16. Gestione commerciale

I Principi di Comportamento di cui al presente paragrafo si riferiscono alle attività di gestione commerciale.

POSSIBILI AREE DI RISCHIO

(i) Negoziazione e gestione dei contratti con qualsiasi soggetto (pubblico o privato);
(ii) Partecipazione a procedure di gara indette da enti pubblici e privati;
(iii) Rapporti con business partner (inclusi partner di joint venture, agenti e intermediari) e gestione dei rapporti di partnership;
(iv) Operazioni finanziarie o commerciali che coinvolgano società del Gruppo Terna concluse con persone fisiche e giuridiche residenti (o con società controllate direttamente o indirettamente da queste) nei Paesi a rischio individuati in Liste di Paesi e/o in Liste di persone fisiche o giuridiche indicate, altresì, dal FATF-GAFI che coordina la lotta contro il riciclaggio di denaro e il finanziamento del terrorismo;
(v) Gestione degli adempimenti doganali.

PRINCIPI DI COMPORTAMENTO

I rapporti con i clienti o i potenziali clienti nonché con i partner commerciali devono essere gestiti in modo corretto, trasparente, equo e cooperativo.

In ogni SE è previsto per i Destinatari il **divieto di**:
- effettuare elargizioni in denaro di propria iniziativa o a seguito di sollecitazione nei confronti di Funzionari Pubblici e/o esponenti della Pubblica Amministrazione, al fine di ottenere un'utilità per la società o per un terzo;
- presentare documentazione che contenga e/o ometta dati, informazioni rilevanti o non veritiere, al fine di far ottenere alla società l'aggiudicazione della gara/commessa;
- affidare lavori, servizi e forniture e disporre i relativi pagamenti senza rispettare i requisiti di forma e tracciabilità richiesti dalle normative vigenti in materia di contratti pubblici e di tracciabilità dei flussi finanziari, ove applicabili;
- effettuare pagamenti o riconoscere compensi in favore di soggetti terzi, senza adeguata giustificazione contrattuale o comunque non adeguatamente documentati, giustificati e autorizzati.

Le Società Estere **dovranno garantire** il rispetto delle procedure adottate dal Gruppo Terna applicabili al processo commerciale (quali le linee guida e/o istruzioni di indirizzo emanate per il Gruppo Terna e le policy locali adottate individualmente da ciascuna Società Estera o dalla relativa controllante, ove applicabili, per la gestione delle attività di export controls (LG061 "Trade Compliance").

Inoltre, nell'ambito di tale processo **è fatto obbligo di**:
- svolgere una Due Diligence nei confronti della controparte in linea con quanto previsto dal par. 13.3;

- improntare tutti i rapporti con le controparti ai principi della trasparenza e dell'integrità e prevedere prestazioni e compensi in linea con le prassi di mercato, accertando che non vi siano aspetti che possano favorire la commissione di Reati in Italia o all'estero;
- nel caso in cui risultino coinvolti nelle operazioni commerciali, in sede di Due Diligence o nella successiva fase di monitoraggio del rapporto commerciale, soggetti i cui nominativi siano contenuti nelle Liste, o i quali siano notoriamente controllati da soggetti contenuti nelle Liste medesime, garantire il rispetto di quanto disciplinato dalla LG070 "Due Diligence su Terze Parti" e dalla LG061 "Trade Compliance";
- verificare che la documentazione e le comunicazioni formali prodotte nel corso di svolgimento della procedura di gara/o attribuzione della commessa siano gestiti e siglati solo dai soggetti preventivamente identificati ed autorizzati dalla SE;
- garantire la tracciabilità delle fasi di formazione delle decisioni e i livelli autorizzativi in modo da essere sempre ricostruibili attraverso gli atti e la documentazione interna;
- definire tutte le partnership e le attività di vendita attraverso rapporti contrattuali, firmati sulla base del sistema di poteri e deleghe in vigore in azienda e comprensivi di clausole in materia di compliance (corporate liability o GCP, Codice Etico, Trade Compliance e procedure in ambito export controls, anticorruzione);
- con particolare riferimento ai contratti con agenti e intermediari, prevedere che questi dovranno anche (i) descrivere chiaramente i servizi che verranno prestati; (ii) definire la natura delle commissioni/provvigioni (fisse, variabili, success fees, ecc.) e il loro ammontare in linea con gli standard di mercato (iii) stabilire i target da raggiungere;
- archiviare tutta la documentazione a supporto delle singole attività.

I principi del libero mercato rientrano tra i valori fondamentali del Gruppo Terna e ne ispirano l'organizzazione e le attività. Pertanto, i comportamenti sono adottati nel rispetto delle regole della leale competizione.

17. Finanza e M&A

I Principi di Comportamento di cui al presente paragrafo si riferiscono al processo di Finanza e M&A e quindi relativo alla gestione dei flussi finanziari e alle operazioni straordinarie (M&A, cessioni, ecc.).

POSSIBILI AREE DI RISCHIO

(i) **Gestione dei flussi finanziari**, per tali intendendosi tutte quelle attività o rapporti che comportano un pagamento o un incasso da o verso la SE, inclusi i cd. rapporti infragruppo;
(ii) **Compimento di operazioni straordinarie** (acquisizioni e cessioni di partecipazioni societarie, fusioni, scissioni, acquisizioni, cessioni e affitti di ramo d'azienda, ecc.).

PRINCIPI DI COMPORTAMENTO

(i) Gestione dei Flussi Finanziari

La gestione dei pagamenti e degli incassi deve avvenire nel rispetto dei seguenti standard minimi:

- i pagamenti devono essere effettuati/ricevuti solo in conformità alla normativa di volta in volta applicabile, alle previsioni contrattuali da cui originano, ai principi contabili in materia di flussi finanziari applicabili;
- tutti i pagamenti devono essere autorizzati nel rispetto delle deleghe e procure rilasciate;
- per quanto possibile, è necessario garantire la segregazione di ruoli e responsabilità dei soggetti coinvolti nel processo dei pagamenti (es. gestione anagrafiche fornitori, benestari, esecuzione materiale del pagamento, etc);
- in ogni caso, le SE non accetteranno e non effettueranno pagamenti:
  - a/da un soggetto diverso dalla controparte contrattuale o
  - da/a conti correnti diversi da quelli previsti contrattualmente o
  - da/a un Paese diverso da quello delle parti o di esecuzione del contratto, senza adeguata giustificazione contrattuale o comunque non adeguatamente documentati, giustificati e autorizzati;
  - da/su conti cifrati o in contanti o strumenti assimilabili[9];
  - nel caso in cui sia indicato/delegato/nominato un soggetto terzo come payer, dovrà essere richiesta la documentazione in merito alla formale individuazione come payer di quel soggetto e le motivazioni sottese a tale interposizione o triangolazione[10];
- è fatto divieto di disporre pagamenti o incassare denaro verso/da Paesi inseriti nelle Liste internazionali senza adeguata documentazione comprovante la reale e specifica necessità;
- deve essere rivolta sempre particolare attenzione ed effettuati gli opportuni controlli relativamente (i) alla sede legale della società controparte (ad es. paradisi fiscali, Paesi a rischio riciclaggio e

[9] La gestione delle transazioni avviene nel rispetto del divieto di utilizzo del contante o altro strumento finanziario al portatore, per qualunque operazione di incasso, pagamento, trasferimento fondi, impiego o altro utilizzo di disponibilità finanziarie; nonché nel rispetto del divieto di utilizzo di conti correnti o libretti di risparmio in forma anonima o con intestazione fittizia. Eventuali eccezioni all'utilizzo di denaro contante o altro strumento finanziario al portatore devono essere espressamente previste dalle procedure della società o del Gruppo Terna applicabili e devono essere scrupolosamente rispettati i limiti all'utilizzo dei contanti previsti dalle normative di riferimento.
[10] A titolo esemplificativo, potranno essere richiesti: (i) un certificato della camera di commercio relativo all'ente pagante; (ii) un documento d'identità del relativo rappresentante legale; (iii) una procura che attesti la delega di pagamento conferita a tale ente pagante; (iv) qualsiasi documento che fornisca il motivo di tale pagamento effettuato dall'ente pagante.

finanziamento del terrorismo, ecc.) ed eventuali schemi societari e strutture fiduciarie utilizzate per transazioni o operazioni straordinarie; (ii) alle transazioni su/da conti correnti accesi presso Paesi a rischio riciclaggio o a finanziamento del terrorismo (di cui alle Liste ad es. GAFI/FATF);
- i controlli sui pagamenti devono contemplare verifiche di coerenza e corrispondenza tra la titolarità del rapporto contrattuale (i.e. il soggetto creditore del pagamento) e l'intestazione del conto su cui effettuare la transazione;
- tutte le operazioni di pagamento/incassi devono essere effettuate con operatori finanziari abilitati che hanno adottato presidi volti a prevenire il fenomeno del riciclaggio;
- in ogni caso, non possono essere effettuati pagamenti in favore di soggetti che non siano chiaramente identificabili;
- in fase di esecuzione dei contratti dai quali derivino flussi finanziari, viene previsto un costante monitoraggio delle transazioni finanziarie effettuate/ricevute. Con particolare riferimento alle operazioni infragruppo, deve essere garantito che le prestazioni rese da/nei confronti delle società del Gruppo Terna siano a condizioni di mercato e regolate da appositi contratti.

(ii) Operazioni straordinarie

Premesso che le SE che intendano porre in essere operazioni straordinarie agiscono in virtù di contratti Intercompany per il tramite di Terna S.p.A, si riepilogano di seguito i Principi di Comportamento da rispettare nello svolgimento delle operazioni di M&A:
- svolgimento di una Due Diligence sulla società target (compresi i rapporti contrattuali in essere della società target) e sulle potenziali controparti che tenga in particolare considerazione il suo profilo etico-reputazionale e, in caso di società, la storia d'impresa e il background della società;
- svolgimento di verifiche circa le implicazioni fiscali derivanti dalle operazioni che si intendono realizzare;
- formalizzazione delle operazioni in contratti scritti inserendo le clausole necessarie ad assicurare il rispetto delle leggi applicabili e delle procedure adottate (corporate liability o GCP, Codice Etico, Trade Compliance e procedure in ambito export controls, anticorruzione) dal Gruppo Terna;
- corretta valutazione, contabilizzazione delle acquisizioni e/o operazioni societarie;
- una volta acquisita una società, dovranno essere poste in essere azioni volte:
  - all'adozione del GCP e pertanto anche al recepimento ed eventuale necessario adeguamento previsto delle procedure vigenti e applicabili nel Gruppo Terna;
  - all'adozione da parte di queste di presidi di controllo il più possibile in linea con quelli gli Standard Generali di Controllo di cui ai par. 13 e ss del presente GCP;
  - alla formazione e/o informazione del relativo personale per l'integrazione.

Tali Principi di Comportamento devono intendersi applicabili a tutti gli incassi e pagamenti nonché, trasversalmente, a tutti i Processi disciplinati dal GCP.

18. Procurement

I Principi di Comportamento di cui al presente paragrafo si riferiscono al processo di procurement.

POSSIBILI AREE DI RISCHIO

(i) Gestione delle procedure di gara/acquisto;
(ii) Affidamento di incarichi professionali e di consulenze;
(iii) Approvvigionamento e catena di fornitura (supply chain).

PRINCIPI DI COMPORTAMENTO

Le SE **devono garantire** che:

- tutti i rapporti con i fornitori siano improntati ai principi della trasparenza e dell'integrità e dell'assenza di conflitti di interessi;
- tutti i rapporti con i fornitori prevedano prestazioni e corrispettivi in linea con le prassi di mercato, accertando l'assenza di termini e modalità che favoriscano la commissione di reati;
- sia assicurata una Due Diligence sui fornitori che tenga in considerazione la loro attendibilità commerciale, reputazionale e professionale;
- nell'ambito dei contratti stipulati con i fornitori, si richieda a loro e ai loro eventuali subappaltatori di rispettare la legislazione internazionale e locale applicabile in materia di lavoro forzato, tutela del lavoro minorile e femminile, e condizioni igienico-sanitarie;
- le relazioni con i fornitori siano formalizzate in contratti scritti che individuino, fra gli altri aspetti:
  - l'oggetto dell'incarico/prestazione e i soggetti che svolgeranno l'incarico o effettueranno la prestazione;
  - l'importo/corrispettivo pattuito e la relativa valuta;
  - il conto corrente presso il quale/dal quale verrà effettuato il pagamento oltre ai termini per la fatturazione (o le modalità di incasso/pagamento) e le condizioni di pagamento;
  - l'impegno del fornitore/consulente a rispettare le leggi nazionali della SE applicabili e le procedure della Società Estera;
  - prevedere una clausola per cui i fornitori si impegnino, nello svolgimento delle attività, al rispetto dei principi del Codice Etico, anche con riguardo all'impegno a non effettuare liberalità che superino il modico valore e che possano essere interpretate come eccedenti le normali pratiche commerciali o di cortesia, o comunque rivolte ad acquisire trattamenti di favore nella conduzione delle attività medesime;
  - prevedere, nei contratti con i Terzi dai quali potrebbe sorgere responsabilità della SE ai sensi della normativa ambientale e della sicurezza sul lavoro, specifiche penali applicabili in caso di violazione, da parte di un fornitore o di un suo subappaltatore, di qualsiasi normativa, internazionale o locale, che tratti le tematiche in parola;
- nel corso di esecuzione del contratto:
  - siano previste le seguenti misure di controllo: (i) aggiornamento periodico della Due Diligence con una frequenza da determinarsi in base al livello di rischio della controparte e/o in caso di revisione/modifica/rinegoziazione del contratto; (ii) attività di monitoraggio della corretta esecuzione del contratto;

- siano rifiutate richieste di controparte relative ad aumenti ingiustificati del corrispettivo o sconti, per questioni non inerenti a modifiche delle condizioni contrattuali, anticipi non previsti a livello contrattuale;
- siano riconosciuti corrispettivi solo previa verifica della corrispondenza tra prestazione ricevuta e previsioni contrattuali;
- i risultati delle attività di selezione, Due Diligence, la documentazione contabile e quella relativa agli accordi contrattuali con il fornitore devono essere registrati e archiviati;
- venga verificata la validità dei pagamenti, controllando che chi riceve o versa importi sia il soggetto indicato nella documentazione contrattuale.

19. Risorse Umane

I Principi di Comportamento di cui al presente paragrafo si riferiscono al processo Risorse Umane.

POSSIBILI AREE DI RISCHIO

(i) Selezione e assunzione del personale;
(ii) Incentivazione del personale e salary review;
(iii) Amministrazione del personale;
(iv) Gestione delle note spese;
(v) Tutela del lavoro e dei diritti dei lavoratori;
(vi) Definizione dei criteri di incentivazione del management delle SE.

PRINCIPI DI COMPORTAMENTO

Nell'ambito della SE deve essere assicurato il rispetto e l'osservanza di tutte le leggi e i regolamenti locali e le procedure della SE in materia di assunzione e gestione delle risorse umane.

In particolare, in ogni SE è previsto quanto segue:

- il divieto di assumere o effettuare promesse di **assunzione di personale** se non in base a necessità aziendali reali e dimostrabili, avvalendosi di un processo di **selezione del personale** che coinvolga almeno due funzioni e che si basi su criteri di oggettività, competenza e professionalità, evitando qualsiasi favoritismo o conflitto di interessi, o qualsiasi azione che si concretizzi in favoritismi, nepotismi o forme clientelari idonee a influenzare l'indipendenza di un Funzionario Pubblico o ad indurlo ad assicurare un qualsiasi vantaggio per la Società Estera o per il Gruppo Terna;
- la **formalizzazione** e la **conservazione** negli archivi aziendali della valutazione dei candidati;
- la chiara **segregazione** delle funzioni coinvolte nelle attività di selezione e assunzione del personale;
- il divieto di **incentivare** mediante promozioni, premi in denaro o altra forma taluni dipendenti, se non sulla base di criteri di oggettività, competenza e professionalità;
- l'adozione di **piani di incentivazione del management** in modo da garantire che gli obiettivi fissati siano tali da non determinare comportamenti abusivi e si concentrino su un risultato ben determinato e misurabile;
- le decisioni riguardanti la **salary review** del personale, **l'avanzamento di carriera** e **l'aumento della retribuzione**, sulla base del merito, delle capacità, della professionalità e dell'esperienza;
- la pianificazione ed erogazione della formazione differenziata a seconda del livello e delle mansioni svolte dai singoli dipendenti;
- che la **documentazione aziendale in materia di etica e compliance**, incluso il GCP, sia resa disponibile agli Esponenti Aziendali mediante pubblicazione sulla rete intranet aziendale o portali della Capogruppo o mediante invio via mail o altre modalità di condivisione di documenti aziendali e che ad ogni neo-assunto sia consegnata e fatta firmare dichiarazione di presa visione (o indicata e messa a disposizione con le modalità sopra individuate) la documentazione in materia di etica e di compliance;

- con riferimento **all'amministrazione del personale**, la corretta predisposizione, registrazione ed archiviazione di tutta la documentazione relativa alla gestione amministrativa del rapporto contrattuale nonché dei trattamenti previdenziali, assicurativi e fiscali del personale, al fine di consentire la ricostruzione delle diverse fasi del processo;
- con riferimento alla **tutela del lavoro e dei diritti dei lavoratori** che siano istituiti dei controlli sugli orari di lavoro volti a prevenire e correggere orari di lavoro eccessivi, che siano garantiti il riposo e work-life balance; siano garantiti salari adeguati e commisurati all'esperienza e alla professionalità del dipendente e siano conformi ai requisiti minimi stabiliti dalla legge prevedendo ulteriormente meccanismi volti a garantire la parità di genere e di retribuzione; l'occupazione e l'inclusione delle persone con disabilità; misure contro la violenza e le molestie sul luogo di lavoro e siano previsti meccanismi volti a vietare il lavoro minorile e il lavoro forzato;
- con riferimento ai **rimborsi delle note spese**, la richiesta dalla funzione competente, prima della liquidazione di tali spese, di appropriata documentazione che includa anche l'originale delle ricevute comprovanti tali esborsi. Tali rimborsi dovranno poi essere accuratamente riportati nei registri contabili delle Società Estere;
- che i dipendenti siano tenuti a **segnalare** qualsiasi situazione che indichi o suggerisca un potenziale conflitto di interessi nell'ambito delle loro attività e qualsiasi potenziale violazione delle suddette politiche e procedure.

20. Amministrazione, Bilancio e Fiscale

I Principi di Comportamento di cui al presente paragrafo si riferiscono al processo Amministrazione, Bilancio e Fiscale.

POSSIBILI AREE DI RISCHIO

(i) Redazione di documenti contabili;
(ii) Gestione delle relazioni con i revisori esterni;
(iii) Gestione della contabilità (attiva e passiva);
(iv) Gestione dei rapporti infragruppo, con specifico riferimento alla gestione dei contratti intercompany;
(v) Gestione degli adempimenti fiscali.

PRINCIPI DI COMPORTAMENTO

Le Società Estere sono tenute a gestire la contabilità in maniera veritiera e corretta.

Il personale operante nell'ambito della **gestione della contabilità** deve svolgere accuratamente le proprie mansioni al fine di **assicurare che**:

a) i dati e le informazioni utilizzate per la preparazione delle relazioni finanziarie periodiche delle SE e dei dati da fornire a Terna S.p.A anche relativi alla normativa europea sulle informazioni di sostenibilità, siano accurati e diligentemente verificati;
b) tutte le voci di bilancio, la cui determinazione e quantificazione sia suscettibile di valutazioni discrezionali, siano quanto più possibile oggettive e supportate da adeguata documentazione;
c) siano previste verifiche volte ad accertare il corretto svolgimento dell'attività di chiusura dei documenti economico/finanziari e, qualora si riscontrino anomalie nelle contabilizzazioni eseguite, prevedere l'obbligo di segnalazione delle stesse alle strutture competenti;
d) tutte le operazioni siano eseguite nel rispetto del sistema autorizzativo adottato;
e) le fatture e l'ulteriore documentazione rilevante in relazione alle operazioni compiute siano accuratamente verificate, registrate e archiviate;
f) le operazioni siano registrate in modo da consentire la predisposizione del bilancio in conformità ai principi contabili applicabili o qualsiasi altro criterio applicabile;
g) l'accesso al relativo archivio documentale sia permesso solo ai soggetti autorizzati in base al sistema autorizzativo in vigore.

Inoltre, alle Società Estere è vietato porre in essere qualsiasi comportamento che impedisca o ostacoli le attività di controllo, di vigilanza e di revisione legale da parte dei revisori esterni attraverso l'occultamento della documentazione o l'uso di altri mezzi fraudolenti.

In ogni SE è previsto il **divieto** di:
- gestire la **fiscalità** in maniera difforme rispetto alla normativa vigente;

- indicare o inviare per l'elaborazione o l'inserimento nelle **comunicazioni**, dati falsi, artefatti, incompleti o comunque non rispondenti al vero, sulla situazione economica, patrimoniale o finanziaria;
- rappresentare in **contabilità** - o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali - dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria;
- registrare in contabilità operazioni con valori non corretti rispetto alla documentazione di riferimento, oppure a fronte di transazioni inesistenti in tutto o in parte, o senza un'adeguata documentazione di supporto che ne consenta, in primis, una corretta rilevazione contabile e, successivamente, una ricostruzione accurata.

Infine, alle Società Estere è richiesto di effettuare in modo corretto, completo, appropriato e tempestivo tutte le comunicazioni verso qualsiasi autorità finanziaria (come previsto dalla legge applicabile locale), non impedendo alle stesse, in alcun modo, di svolgere i propri compiti anche in occasione di qualsiasi ispezione.

In relazione ai rapporti infragruppo, le attività devono essere disciplinate da appositi contratti di service formalizzati. Inoltre, le transazioni con le società del Gruppo Terna devono essere valutate per assicurare (a) la convenienza tecnica ed economica dell'operazione, (b) che la valutazione dell'ammontare economico delle prestazioni sia effettuata al valore di mercato effettivo e (c) che il rapporto contrattuale sia sostanzialmente conforme alle operazioni commerciali in effetti realizzate e alla loro rappresentazione contabile.

21. Gestione delle informazioni riservate e privilegiate

I Principi di Comportamento di cui al presente paragrafo si riferiscono al processo Gestione delle Informazioni Riservate e Privilegiate.

POSSIBILI AREE DI RISCHIO

(i) Gestione dei rapporti ed incontri con gli investitori, con gli analisti finanziari, con i media ed in generale gestione dell'informativa pubblica;
(ii) Gestione dei contenuti aziendali pubblicati sul sito internet aziendale e social media e organizzazione di eventi;
(iii) Gestione delle informazioni aziendali riguardanti la SE o altre società del Gruppo Terna, comprese le Informazioni Privilegiate, che non siano di pubblico dominio e che per oggetto o per altre caratteristiche abbiano comunque carattere riservato verso soggetti non tenuti ad obblighi di riservatezza in base alla normativa vigente o per accordi contrattuali ("Informazioni Riservate"), come individuate dalla LG005 "Procedura per la gestione, il trattamento e la comunicazione delle informazioni aziendali relative a Terna S.p.A. e alle società controllate";
(iv) Gestione delle informazioni classificabili come informazioni Privilegiate riferite a Terna e ai relativi strumenti finanziari individuate dalla LG005 "Procedure per la gestione, il trattamento e la comunicazione delle informazioni aziendali relative a Terna S.p.A. e alle società controllate";
(v) Ogni genere di transazione sugli strumenti finanziari quotati in portfolio del Gruppo Terna.

PRINCIPI DI COMPORTAMENTO

La gestione delle Informazioni Riservate e/o Informazioni Privilegiate è garantita nel rispetto delle procedure valevoli per il Gruppo Terna in materia di market abuse (rif. LG005 e LG008) nonché in conformità alle normative comunitarie e locali in materia.

Gli Esponenti Aziendali delle SE **si impegnano**:

- a non esprimere opinioni, rilasciare dichiarazioni o fornire informazioni ai media per conto della SE o di società del Gruppo Terna al di fuori dei canali e delle modalità stabilite in ambito aziendale, adottando ogni necessaria cautela affinché la relativa circolazione nel contesto aziendale possa svolgersi senza pregiudizio del carattere riservato/privilegiato/potenzialmente privilegiato delle informazioni stesse e secondo il principio del c.d. *need to know* e tenendo conto degli indirizzi di cui alla LG005 ;
- affinché l'organizzazione degli eventi aziendali dedicati agli organi di informazione sia regolata in modo tale da evitare l'offerta di doni o forme di intrattenimento che possano influenzare l'obiettività di giudizio e l'indipendenza degli organi di informazione partecipanti;
- affinché i rapporti con agenzie di rating e società di certificazione siano limitati allo scambio di informazioni che si ritenga necessario – sulla base delle previsioni contrattuali pattuite – per l'adempimento dell'incarico, evitando qualsiasi condotta potenzialmente idonea a lederne l'indipendenza.

Per gli Esponenti Aziendali della SE è previsto il **divieto di**:

- servirsi di Informazioni Privilegiate per negoziare, direttamente o indirettamente, strumenti finanziari al fine di ottenere vantaggio personale o per favorire soggetti terzi o una società del Gruppo Terna;
- raccomandare o indurre qualcuno, sulla base di Informazioni Privilegiate, a porre in essere transazioni su strumenti finanziari;
- rivelare Informazioni Riservate, Informazioni potenzialmente privilegiate o Privilegiate a soggetti terzi, salvo che ciò sia richiesto da un'Autorità Pubblica o stabilito in specifici contratti in virtù dei quali la controparte sia vincolata ad utilizzare le informazioni solo per lo scopo previsto e a mantenerne la segretezza;
- diffondere informazioni false o fuorvianti (siano esse relative alla SE/qualsiasi altra società del Gruppo Terna) tramite i media, internet, o altro mezzo, al fine di alterare il prezzo di mercato di strumenti finanziari;
- porre in essere qualsiasi condotta o transazione su strumenti finanziari che sia contraria alla disciplina relativa ai reati di market abuse prevista dalla normativa applicabile e declinata nelle LG005 e LG008;
- accedere abusivamente al sistema informatico o telematico aziendale al fine di alterare e/o cancellare dati o informazioni;
- inviare attraverso un sistema informatico aziendale informazioni o dati falsificati o, in qualunque modo, alterati.

22. Health, Safety and Environment ("HSE")

I Principi di Comportamento di cui al presente paragrafo si riferiscono al processo Health, Safety and Environment ("HSE").

POSSIBILI AREE DI RISCHIO

(i) Gestione degli adempimenti in tema di salute e sicurezza e ambiente;
(ii) Gestione di situazioni di potenziale contaminazione di suolo, sottosuolo, acque superficiali e sotterranee;
(iii) Gestione e smaltimento rifiuti;
(iv) Emissioni in atmosfera;
(v) Scarichi idrici;
(vi) Gestione infortuni e malattie professionali;
(vii) Gestione dei cantieri;
(viii) Selezione dei Terzi e gestione dei relativi rapporti nell'ambito delle attività in materia di salute, sicurezza e ambiente.

PRINCIPI DI COMPORTAMENTO

A) Salute e Sicurezza nei Luoghi di Lavoro
Indipendentemente dall'ampiezza della legislazione locale in materia di salute e sicurezza sul luogo di lavoro, la SE è tenuta a promuovere un'efficace cultura della protezione della sicurezza sul luogo di lavoro, favorendo la consapevolezza in merito ai rischi e alle responsabilità delle condotte dei singoli. La promozione della salute e sicurezza sul lavoro, infatti, non costituisce solo un obbligo normativo, ma rappresenta un valore etico e sociale fondamentale per l'organizzazione, che si traduce in un impegno concreto volto a garantire condizioni di lavoro sicure e salutari per tutti i lavoratori.

Le SE devono tenere in considerazione la sicurezza dei lavoratori attraverso ogni fase dell'attività e devono impegnarsi ad adottare tutte le misure considerate necessarie al fine di proteggere l'integrità fisica e morale dei propri lavoratori.

In particolare, la SE **deve**:
a) considerare il rispetto delle previsioni di legge in materia di salute e sicurezza dei lavoratori sul luogo di lavoro quale una priorità e attribuire a tal fine le risorse economiche necessarie;
b) responsabilizzare l'organizzazione aziendale al fine di evitare che l'attività di prevenzione venga considerata di competenza esclusiva di alcuni soggetti;
c) identificare correttamente i requisiti richiesti in materia di salute e sicurezza sui luoghi di lavoro da leggi e regolamenti locali;
d) per quanto possibile e permesso dall'evoluzione delle migliori pratiche, valutare i rischi per i lavoratori allo scopo di proteggerli, anche adottando i materiali e l'attrezzatura più adeguati, al fine di ridurre il rischio alla radice;

e) impegnarsi al miglioramento continuo e alla prevenzione, valutando correttamente quei rischi che non sono evitabili e mitigarli adeguatamente tramite l'implementazione di appropriate misure di sicurezza individuali e collettive (es.: fornire dispositivi di protezione individuali adeguati alle mansioni svolte; dotare l'area di lavoro di un kit di pronto soccorso);
f) garantire un'adeguata sorveglianza sanitaria, come strumento essenziale per la tutela della salute dei lavoratori nel lungo periodo;
g) diffondere informazioni in merito alla salute e sicurezza sul luogo di lavoro, aggiornate e specifiche con riferimento alle attività esercitate, assicurando che i lavoratori siano correttamente istruiti e formati;
h) assicurare che i lavoratori siano coinvolti in attività di formazione e aggiornamenti periodici e specifici in merito ai temi relativi alla salute e sicurezza sul luogo di lavoro ed effettuare adeguate attività di monitoraggio per la gestione, rettifica, inibizione di comportamenti posti in violazione delle norme;
i) assicurare che i piani di incentivazione del management siano adottati in modo da garantire che gli obiettivi fissati siano tali da non determinare comportamenti abusivi e si concentrino su un risultato ben determinato e misurabile;
j) prendere in considerazione e analizzare ogni episodio di mancato rispetto della normativa o area di miglioramento, emersa come tale a seguito dell'attività lavorativa o durante ispezioni;
k) promuovere, ove possibile, iniziative volte a favorire il benessere psicofisico dei lavoratori, in un'ottica di prevenzione e sostenibilità sociale;
l) considerare la salute e sicurezza come parte integrante della responsabilità sociale dell'impresa strutturando l'organizzazione dell'attività di lavoro al fine di proteggere l'integrità dei lavoratori, dei Terzi e della comunità nel cui ambito la SE opera.

Inoltre, con particolare riferimento alla selezione di Terzi coinvolti nella gestione degli aspetti inerenti alla salute e sicurezza nei luoghi di lavoro, la SE **deve garantire**:
- la verifica dell'idoneità tecnica-professionale del Terzo e la sua conformità alle normative applicabili in materia di salute e sicurezza;
- l'integrazione di criteri di sostenibilità e responsabilità sociale nella selezione e nella valutazione del Terzo, favorendo pratiche di lavoro sicure ed etiche.
- la stipula di un contratto che includa clausole specifiche per la conformità normativa prevedendo anche specifiche penali in caso di violazione, da parte del fornitore o del suo subappaltatore, di qualsiasi normativa, internazionale o locale, applicabile in materia di salute e sicurezza nei luoghi di lavoro;
- la gestione delle problematiche connesse a sicurezza e analisi dei rischi;

Al fine di mantenere un corretto monitoraggio delle Aree a Rischio, ciascuna SE alloca risorse organizzative, strumentali ed economiche per assicurare, da un lato, il pieno rispetto delle previsioni di legge sulla prevenzione degli incidenti sul luogo di lavoro e, dall'altro lato, il continuo miglioramento della situazione relativa alla salute e alla sicurezza sul luogo di lavoro, anche tramite l'implementazione e l'aggiornamento delle relative misure precauzionali.

Gli Esponenti Aziendali devono cooperare al fine di garantire il pieno rispetto delle disposizioni di legge, delle procedure aziendali e di ogni altra normativa interna volta a proteggere la sicurezza e la salute dei lavoratori sul luogo di lavoro.

B) Ambiente

La SE considera il rispetto e la protezione dell'ambiente una priorità e, in particolare:

a) diffonde nella società informazioni riguardo alla protezione dell'ambiente con riferimento alle attività esercitate, promuovendo la consapevolezza di tale tematica e assicurando che le attività vengano svolte nel rispetto della normativa applicabile;
b) identifica correttamente i requisiti richiesti in materia ambientale da leggi e regolamenti locali e valuta i rischi ambientali connessi alle principali attività condotte, nonché connessi intrinsecamente ai propri impianti;
c) adotta strumenti adeguati al fine di impedire che le attività aziendali causino qualsivoglia forma di pregiudizio o danno all'ecosistema (es. dovuti ad una non corretta gestione dei rifiuti prodotti o all'inquinamento da sostanze pericolose e dannose per l'ambiente o al mancato rispetto di habitat protetti) introducendo altresì misure di prevenzione del danno ambientale nonché di protezione per mitigare lo stesso;
d) effettua adeguate attività di monitoraggio per la gestione, rettifica, inibizione di comportamenti posti in violazione delle norme;
e) assicura che i piani di incentivazione del management siano adottati in modo da garantire che gli obiettivi fissati siano tali da non determinare comportamenti abusivi e si concentrino, invece, su un risultato ben determinato e misurabile;
f) si adopera per una gestione dei rifiuti orientata al recupero, al reimpiego e al riciclaggio dei materiali, al fine di garantire un maggior grado di protezione della salute dell'ambiente e quindi anche dell'uomo in termini più generali promuove una strategia di economia circolare puntando a raggiungere una rilevante performance ambientale.

Nella selezione di Terzi coinvolti nella gestione degli aspetti ambientale, la SE **deve garantire**:

- la verifica dell'idoneità tecnica-professionale del Terzo;
- la stipula di un contratto che preveda anche specifiche penali applicabili in caso di violazione, da parte del fornitore o di un suo subappaltatore, di qualsiasi normativa, internazionale o locale nonché ulteriore normativa stabilita da Terna e condivisa contrattualmente con i Terzi, applicabile in materia ambientale;
- la gestione delle problematiche connesse alle tematiche ambientali.

23. Information & Communications Technology ("ICT")

I Principi di Comportamento di cui al presente paragrafo si riferiscono al processo Information & Communications Technology ("ICT").

POSSIBILI AREE DI RISCHIO

i. Gestione dei sistemi informativi aziendali al fine di assicurarne il funzionamento e la manutenzione, l'evoluzione della piattaforma tecnologica e applicativa IT nonché la sicurezza informatica, fisica e logica; ivi incluse:

a. la gestione dell'attività di manutenzione dei sistemi esistenti e gestione dell'attività di elaborazione dei dati;

b. ogni attività aziendale compiuta utilizzando intranet, internet, il sistema di posta elettronica o ogni altro strumento informatico;

c. la gestione e la protezione delle postazioni di lavoro, dei computer portatili, dei telefoni cellulari e delle unità di archiviazione;

d. la programmazione delle misure da adottare sui sistemi telematici nonché della protezione, classificazione e trattamento delle informazioni e dei dati.

PRINCIPI GENERALI DI COMPORTAMENTO

Ogni Esponente Aziendale **si astiene** dal commettere le seguenti condotte:

- la manomissione o l'alterazione del sistema informatico e/o dei documenti informatici della SE;
- l'illegittimo accesso di soggetti terzi al sistema informatico;
- un uso improprio delle credenziali informatiche;
- l'intervenire illegalmente con qualsiasi modalità su dati, informazioni o programmi informatici;
- la condivisione non autorizzata di informazioni commerciali al di fuori dall'azienda e l'utilizzo di dispositivi personali o non autorizzati per trasmettere o archiviare informazioni o dati aziendali (es.: divulgare, cedere o condividere le proprie credenziali di accesso ai sistemi e alla rete aziendale della società o di Terzi; accedere abusivamente al sistema informatico di Terzi);
- lo sfruttamento di falle nelle misure di sicurezza del sistema informatico aziendale al fine di ottenere accesso a informazioni in assenza della dovuta autorizzazione;
- l'installazione o modificazione di software o banche dati o hardware in assenza di preventiva autorizzazione;
- l'utilizzo di software non autorizzati o di hardware che possano essere impiegati per compromettere la sicurezza di sistemi informatici (quali software per identificare le credenziali, decrittare file criptati, ecc.);
- il mascherare, oscurare o sostituire la propria identità e inviare e-mail riportanti false generalità o inviare intenzionalmente e-mail contenenti virus o altri programmi in grado di danneggiare o intercettare dati;
- l'accedere abusivamente al sito internet della SE al fine di manomettere o alterare abusivamente qualsiasi dato ivi contenuto ovvero allo scopo di immettervi dati o contenuti

multimediali (immagini, infografica, video, ecc.) in violazione della normativa sul diritto d'autore e delle procedure aziendali applicabili;
- il lasciare gli strumenti informatici in dotazione, come personal computer o Smartphone, incustoditi o sbloccati quando non in uso;
- l'apertura di e-mail o allegati sospetti ricevuti via posta elettronica o altro mezzo di comunicazione. In tal caso dovrà segnalare alla struttura di cybersecurity di riferimento qualsiasi comunicazione sospetta.

Pertanto, la SE assicura, tramite l'implementazione di adeguate misure organizzative, tecniche e fisiche, la prevenzione delle condotte sopra descritte anche attraverso (a) la gestione sicura dei sistemi informativi e (b) la gestione efficace del ciclo di vita di ogni applicativo aziendale.

A) Gestione sicura dei sistemi informativi

La SE, al fine di garantire adeguati presidi di sicurezza informatica, assicura conformità al Framework NIST e, in particolare, agli ambiti definiti dal CSF 2.0.
In tale contesto, la SE assicura:

- **in ambito GOVERN**:
  - la presenza di un modello di governance della sicurezza che contempli il rischio di cyber security;
  - l'individuazione di ruoli, responsabilità e dei relativi poteri inerenti alla sicurezza informatica;
  - la verifica e la revisione continua dell'attuazione delle attività legate alla gestione del rischio di cyber security;
  - l'integrazione del rischio di cyber security della catena di approvvigionamento all'interno del rischio dell'organizzazione;
- **in ambito IDENTIFY**:
  - l'identificazione e il censimento degli asset informatici aziendali attraverso appositi inventari;
  - la valutazione e il trattamento del rischio di cyber security al quale i sistemi informativi aziendali sono esposti, nonché la gestione dei piani di rientro definiti;
  - l'identificazione, la registrazione e la risoluzione delle vulnerabilità tecnologiche dei sistemi informativi aziendali;
  - la valutazione delle performance e il miglioramento continuo di processi, procedure e attività di gestione del rischio di cyber security dell'organizzazione.
- **in ambito PROTECT**:
  - la limitazione degli accessi agli asset fisici e logici dell'organizzazione ai soli utenti autorizzati;
  - la diffusione e la promozione di competenze e consapevolezza in materia di cyber security mediante specifiche iniziative di sensibilizzazione e formazione del personale;
  - la protezione della riservatezza, dell'integrità e della disponibilità dei dati a riposo, in transito e in uso, anche mediante la predisposizione di copie di backup dei dati informatici presenti sui sistemi aziendali;
  - la configurazione e la manutenzione di hardware, software e servizi delle piattaforme fisiche e virtuali secondo principi di sicurezza;
  - l'installazione e l'utilizzo di strumenti hardware e software approvati da attori interni all'organizzazione;

- l'adozione di pratiche di sviluppo sicuro del software;
- l'utilizzo di strategie tecniche e operative per garantire la resilienza dei sistemi in situazioni normali e avverse;
- la sicurezza delle reti informative;

➢ **in ambito DETECT**:
- il monitoraggio continuo e l'analisi di anomalie ed eventi di cyber security potenzialmente avversi;

➢ **in ambito RESPOND**:
- la gestione degli incidenti di cyber security mediante un processo strutturato che includa fasi di identificazione, analisi e risposta;

➢ **in ambito RECOVER**:
- la disponibilità operativa dei sistemi e dei servizi interessati da incidenti di cyber security, attraverso l'esecuzione di attività di ripristino e test di integrità sulle copie di sicurezza.

B) Principi di sviluppo del codice e delle applicazioni

La gestione del ciclo di vita applicativo (SDLC) rappresenta un insieme strutturato di processi, attività e strumenti finalizzati a garantire che le soluzioni software vengano progettate, sviluppate, testate, rilasciate e mantenute in modo efficace, sicuro e scalabile.

Lo sviluppo applicativo deve seguire principi che garantiscano sicurezza, tracciabilità, qualità e interoperabilità.
È fondamentale pertanto adottare un approccio metodologico che assicuri coerenza tra requisiti funzionali e tecnici, tracciabilità delle modifiche, qualità del codice e governance operativa con particolare attenzione alla progettazione di tutti gli strumenti a supporto della gestione delle applicazioni tanto quanto la progettazione delle applicazioni stesse. Ogni fase del ciclo – dall'analisi iniziale fino al monitoraggio post-rilascio – deve essere supportata da strumenti e processi integrati (come CMDB, soluzioni di Osservabilità, piattaforme di IT Service Management, pipeline CI/CD, sistemi di test e reporting). Questo approccio consente di ridurre i rischi, migliorare la qualità dei rilasci, ottimizzare i tempi di delivery e garantire la continuità dei servizi IT.

Una gestione efficace del ciclo di vita applicativo è quindi un elemento chiave per l'evoluzione digitale e la resilienza delle piattaforme applicative aziendali.

Secondo tali principi le seguenti attività devono essere svolte per ciascuna iniziativa di sviluppo applicativo:
- **Analisi di impatto e valutazione dei rischi**: Prima dell'avvio progettuale, è essenziale analizzare l'impatto sui sistemi esistenti e valutare i rischi tecnici, operativi e di sicurezza. Questo consente di pianificare correttamente le attività e mitigare potenziali criticità.
- **Definizione e tracciabilità dei requisiti funzionali**: I requisiti funzionali devono essere raccolti in modo strutturato e tracciabile, garantendo allineamento con gli obiettivi di business e facilitando la verifica e la validazione lungo tutto il ciclo di vita.
- **Derivazione dei requisiti tecnici**: Dai requisiti funzionali si estraggono quelli tecnici, necessari per definire architettura, componenti, interfacce e dipendenze. Questa fase assicura che la soluzione

sia scalabile, sicura e integrabile. Le architetture e i pattern di integrazione devono essere analizzati e validati al fine di garantire robustezza e massimizzare il riutilizzo.

- **Gestione della configurazione e del versionamento:** L'uso di sistemi di version control (es. Git) e ambienti segregati consente di gestire in modo sicuro il codice, le configurazioni e le dipendenze, garantendo tracciabilità e possibilità di rollback.
- **Sviluppo dell'applicazione e dei test**: Lo sviluppo deve seguire standard di codifica e includere la progettazione dei test fin dalle prime fasi. I test (unitari, di integrazione, funzionali) devono essere automatizzati e versionati per garantire qualità e ripetibilità. Laddove possibile è preferibile scrivere delle routine di test scriptabili.
- **Continuous Integration / Continuous Delivery (CI/CD):** Le pipeline CI/CD automatizzano build, test e rilascio, riducendo gli errori manuali e accelerando il time-to-market. Devono essere integrate con sistemi di controllo qualità e sicurezza.
- **Esecuzione dei test**: I test devono essere eseguiti in ambienti controllati, con evidenze documentate e criteri di accettazione definiti. Il superamento dei test è prerequisito per il rilascio in produzione.
- **Gestione del rilascio in esercizio**: Il rilascio in produzione deve essere governato da processi di release management, con piani di deployment, rollback e comunicazione. È fondamentale il coordinamento tra team IT e il business per garantire una transizione fluida.
- **Configurazione dei sistemi di supporto della gestione e manutenzione delle applicazioni post rilascio**: Contestualmente al rilascio, è necessario aggiornare CMDB, ITSM, strumenti di monitoraggio, logging e reporting. Questi sistemi garantiscono visibilità, tracciabilità e capacità di intervento tempestivo nelle fasi successive al rilascio.
- **Monitoraggio post-rilascio e gestione delle metriche**: In produzione, l'applicazione deve essere monitorata costantemente per rilevare anomalie e degradazioni. Le metriche operative (es. uptime, error rate, performance) supportano l'esecuzione di processi di manutenzione evolutiva e correttiva a livello infrastrutturale e applicativo.
- **Gestione delle modifiche e del ciclo evolutivo**: Le evoluzioni applicative devono essere gestite tramite processi di Change Management, con analisi di impatto, approvazioni e aggiornamenti documentali. Questo garantisce continuità e controllo.

In aggiunta alle buone pratiche SDLC è necessario che le soluzioni SW sviluppate siano integrabili con i processi e le soluzioni di Terna. Pertanto, sin dalla fase di disegno e progettazione di ogni soluzione SW è imprescindibile valutare la possibilità di condivisione automatica dei dati e l'interoperabilità dei processi tra ciascuna SE e Terna. Per garantire uniformità di comportamento Terna detterà i momenti, nell'ambito dell'esecuzione del processo di business, in cui l'integrazione dovrà avvenire, il tracciato record e le modalità standard di interfacciamento con ciascuna delle controllate. Testato e certificato il canale e l'interfaccia di trasmissione dei dati, la responsabilità del dato rimane in capo alla società in carico alla produzione dello stesso.

24. Allegati

- a01LG058 Appendice A - Reati
- a02LG058 Appendice B - Flussi informativi
- a03LG058 Appendice C - Sistema di controllo interno