INFRATEL ITALIA

INVITALIA

Modello di Organizzazione,

Gestione e Controllo

Parte speciale

ai sensi del D.Lgs. 231/01

Infratel Italia S.p.A.
Sede Legale: Via Calabria, 46 - 00187 Roma
T +39 06 97749311 F +39 06 97749370
www.infratelitalia.it
Iscrizione al Registro delle Imprese di Roma
R.E.A. 1055521 - C.F. e P.IVA 07791571008

Sede Operativa:
Via Silvio D'Amico 40 – 00145 Roma
posta@pec.infratelitalia.it
infrastruttureservizidigitali@postacert.infratelitalia.it
italiadomanipnrr@postacert.infratelitalia.it

Società soggetta alla direzione ed al coordinamento
dell'Agenzia nazionale per l'attrazione degli investimenti
e lo sviluppo d'impresa S.p.A. - INVITALIA
Azionista Unico - Capitale sociale € 8.594.044,00

Consiglio di Amministrazione del 18 marzo 2025

CAPITOLO I DEFINIZIONI E PRINCIPI GENERALI. INTEGRAZIONE E COORDINAMENTO DEI SISTEMI DI GESTIONE

I.1 FINALITÀ E DESTINATARI DEL MODELLO

La presente Parte Speciale del Modello di Organizzazione Gestione e Controllo, redatto ai sensi del D.Lgs. 231/01 (il "Modello 231 – Parte Speciale"), ha lo scopo di definire le regole di gestione ed i principi di comportamento che tutti i destinatari dovranno seguire al fine di prevenire – nell'ambito delle specifiche attività svolte in Infratel Italia S.p.A. (di seguito "Infratel Italia" o la "Società") e considerate "a rischio" – la commissione dei reati previsti dal D.Lgs. 231/01 e dalla L. 190/2012, oltre ad assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali con specifico riferimento a quanto previsto dal D.Lgs. 33/2013 e s.m.i., dal D.Lgs. 39/2013 e dal D.lgs. 36/2023, per quanto di rilievo[1].
Il seguente documento ha lo scopo di:

- indicare le regole che i destinatari sono chiamati ad osservare ai fini della corretta applicazione del Modello 231, Parte Generale e Parte Speciale;
- fornire all'Organismo di Vigilanza (OdV), al Responsabile dell'attuazione del Piano di Prevenzione della Corruzione e della Trasparenza (RPCT) e alle altre funzioni di controllo, i principi e gli schemi concettuali per esercitare le attività di monitoraggio, controllo e verifica, che dovranno essere implementate nelle procedure, nelle istruzioni operative, nei regolamenti, nelle policies e nei moduli della Società.

In linea generale, tutti i destinatari dovranno adottare, ciascuno per gli aspetti di propria competenza, comportamenti conformi alle determinazioni contenute nel Modello 231, Parte Generale e Parte Speciale, ai sensi del D.Lgs. 231/01, di Infratel Italia, che si compone di:

- Codice Etico
- Parte Generale
- Parte Speciale (suddivisa in capitoli)
- Allegato A – Appendice normativa (testo del decreto e delle disposizioni penali ivi richiamate)
- Allegato B – Disposizione organizzativa
- Allegato C – Mappa dei processi, delle unità organizzative e degli ambiti
- Allegato D – Schema del sistema di controlli interni
- Allegato E – Matrice rischi – soggetti – processi
- Allegato F – Flussi verso l'Organismo di Vigilanza
- Allegato G – Piano di Prevenzione della Corruzione

Ogni altro elemento della normativa aziendale (procedure organizzative, regolamenti, policies, istruzioni operative, moduli – la "Normativa Aziendale") dovrà essere definito in coerenza e nel rispetto dei principi di controllo espressi nel Modello 231, Parte Generale e Parte Speciale di Infratel Italia. È inoltre espressamente vietato adottare comportamenti contrari a quanto previsto dalle vigenti norme di legge.
Le regole contenute nel Modello 231, Parte Generale e Parte Speciale di Infratel Italia si applicano a coloro che svolgono, anche di fatto, funzioni di rappresentanza, amministrazione, direzione o controllo della Società, a tutti i dipendenti, ai lavoratori subordinati della Società, di qualsiasi grado e in forza di qualsivoglia tipo di rapporto contrattuale.
Il Modello 231, Parte Generale e Parte Speciale si applica altresì, nei limiti del rapporto in essere, a coloro i quali, pur non appartenendo alla Società, operano su mandato o per conto della stessa, in particolare per ciò che concerne le attività svolte per Infratel Italia dalle funzioni/uffici di Invitalia S.p.A. (la "Capogruppo") in virtù del contratto di service, o per i soggetti che sono comunque legati ad Infratel Italia da rapporti giuridici rilevanti in relazione alla possibile configurazione dei reati contemplati dal D.Lgs. 231/01 e dalla L.190/2012. I soggetti con

[1] In particolare, si veda l'art. 1, comma 2-bis L. 190/2012, in forza del rinvio operato dall'art. 2-bis, d.lgs. 33/2013, stante il suo rilievo "ai fini dell'adozione di misure di prevenzione della corruzione integrative di quelle adottate ai sensi del d.lgs. 8.6.2001, n. 231". Si vedano altresì l'art. 3, comma 1, lett. a), D.lgs. 39/2013 e l'art. 13 D.Lgs. 36/2023.

cui Infratel conclude rapporti contrattuali, ivi inclusi i consulenti esterni, i tirocinanti ed i collaboratori a qualsiasi titolo coinvolti nelle attività di Infratel Italia, non soggetti al vincolo della subordinazione, sono comunque tenuti al rispetto del Modello in forza di clausole appositamente redatte all'atto della stipula dei relativi contratti.
I destinatari del Modello 231, Parte Generale e Parte Speciale sono tenuti a rispettare con la massima correttezza e diligenza tutte le disposizioni ivi contenute, nonché tutte le procedure di attuazione delle stesse.

I.2 LE "AREE A RISCHIO REATO", LE "ATTIVITÀ SENSIBILI", LE "ATTIVITÀ STRUMENTALI" E GLI ELEMENTI DI CONTROLLO

I.2.1. ATTIVITÀ SENSIBILI E STRUMENTALI

L'art. 6, comma 2, lett. a) del D.Lgs. 21/01 indica, come uno degli elementi essenziali dei modelli di organizzazione, gestione e controllo previsti dal decreto, l'individuazione delle cosiddette attività "sensibili", ossia quelle attività aziendali nel cui ambito potrebbe concretizzarsi il rischio di realizzazione della condotta illecita espressamente richiamata dal decreto.
Al fine di ottemperare a quanto disposto dal D.Lgs. 231/01 2, Infratel Italia ha posto in essere le seguenti attività:

- analisi delle aree di attività di ciascuna funzione aziendale, mediante interviste dirette e/o invio di questionari ai responsabili delle funzioni e delle aree di business della Società;
- individuazione e mappatura delle aree "a rischio reato", delle attività "sensibili" e di quelle "strumentali" relative a ciascuna funzione aziendale;
- analisi del profilo di rischio, per ciascuna attività "sensibile", mediante individuazione dei reati potenzialmente realizzabili;
- analisi delle modalità di realizzazione delle condotte illecite;
- identificazione dei processi aziendali di riferimento nell'ambito dei quali devono essere previsti i controlli a presidio dei rischi individuati.

È stata successivamente svolta un'analisi dettagliata di ciascuna singola attività, finalizzata a verificarne i contenuti, le concrete modalità operative, la ripartizione delle responsabilità, nonché la sussistenza di ciascuna delle ipotesi di reato indicate dal D.Lgs. 231/01 e dalla L.190/2012.

A seguire si riportano, per ciascuna area/macro processo aziendale, le attività "sensibili" e/o "strumentali" individuate. Le attività "sensibili" sono quelle direttamente esposte al rischio di commissione del reato. Un processo viene definito meramente "strumentale" laddove le attività che lo compongono non risultano invece direttamente "esposte" alla possibilità di commissione del reato, ma sono caratterizzate da situazioni che possono assumere carattere di supporto indiretto e dunque agevolare la commissione di determinati reati, commessi da un'altra area aziendale. A questi sono associati **specifici elementi di controllo.** Dei rischi strumentali sottostanti alle aree a rischio diretto e delle attività meramente strumentali (come meglio specificate in seguito, nelle tabelle), che non sono obiettivo specifico di prevenzione dell'area di competenza, il *management* aziendale ed i vertici societari tengono conto al fine del miglioramento del sistema di controllo interno, con l'attenzione necessaria per individuare e risolvere possibili interdipendenze o sfere di eccessiva discrezionalità, funzionali ad agevolare la commissione dei reati previsti dal Decreto, attraverso misure generali di redistribuzione o rotazione dei ruoli, ovvero di miglioramento dei presidi specifici di controllo.
Una più dettagliata evidenza di tali elementi specifici di controllo è inoltre delegata all'intero corpo normativo aziendale (policies, regolamenti, procedure, istruzioni operative, moduli).

I.2.2. ELENCO REATI DI REMOTA POSSIBILITÀ DI VERIFICAZIONE ED ELENCO DEI REATI A PROBABILITÀ DI VERIFICAZIONE DIFFUSA

L'attività di *risk assessment* ha condotto all'esclusione dei seguenti reati, perché considerati difficilmente configurabili in relazione agli scopi sociali e alle altre caratteristiche di Infratel Italia.

Art. 25-quater D.lgs. 231/2001 - Reati con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali
Art. 25-quater.1 D.lgs. 231/2001 - Pratiche di mutilazione degli organi genitali femminili
Art. 25-terdecies D.lgs. 231/2001 - Razzismo e xenofobia
Art. 25-quaterdecies D.lgs. 231/2001 - Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati
Art. 25-sex decies D.lgs. 231/2001 - Contrabbando

Al contempo, è opportuno rilevare che due tipologie di fattispecie previste dal Decreto sono invece di possibile verificazione indistintamente in ogni area operativa. Si tratta, in particolare, dei seguenti delitti:

Art. 25-septies, D.lgs. 231/2001 - delitti commessi in violazione della normativa a tutela della salute e sicurezza sui luoghi di lavoro
Art. 24-ter D.lgs. 231/2001 - delitti associativi

I primi, in ragione del fatto che ogni lavoratore/destinatario del MOGC 231 è soggetto al pericolo di infortunio/malattia lavorativa. I secondi in ragione della loro natura intrinsecamente plurisoggettiva e pervasiva.
Infine, va rammentato, sebbene non si ravvisino ragioni di una mappatura specifica di tali rischi, che i fatti di cui al Decreto possono essere consumati nella forma tentata e possono avere rilievo anche transnazionale (art. 26 D.lgs. 231/2001 e L. 146/2006).
Essendo il rischio diffuso, le misure organizzative in materia di prevenzione infortuni e malattie professionali vanno riferite a tutti i destinatari del Modello. Per i rischi relativi ai delitti associativi, si osservano i protocolli generali, con particolare attenzione alla misura della rotazione.

I.2.3. STRUTTURA ORGANIZZATIVA

Le **unità organizzative** che riportano **all'Amministratore Delegato** (processi gestionali e di supporto di secondo livello) corrispondono ai seguenti uffici:

- **Controllo di Gestione;**

- **Acquisti, Affari Generali e Demand Organizzazione**, gestore dell'omonimo macro-processo/funzione, al cui riporto sono articolate l'unità organizzativa **Demand Organizzazione e Affari Generali** (suddivisa negli ambiti **Affari Generali** e **Demand Organizzazione**) e l'ambito **Acquisti**;

- **Qualità, Privacy e Sicurezza**, gestore dell'omonimo macro-processo/funzione, al cui riporto sono articolate l'unità organizzativa **Verifiche Cantieri** e l'ambito **Privacy, SSL e Qualità**. Il responsabile dell'ufficio "Qualità, Privacy e Sicurezza" è altresì il Delegato del Datore di Lavoro per le funzioni relative alla Salute e Sicurezza sui luoghi di Lavoro (*ex* art. 16 TUSL), per la gestione degli aspetti ambientali e per la nomina e la revoca dei responsabili del trattamento dati;

- **Pianificazione, Gare e Ingegneria**, gestore dell'omonimo macro-processo/funzione, al cui riporto sono articolate le unità organizzative **Pianificazione**, **Gare e Assistenza RUP**, **Ingegneria delle Reti e dei Sistemi**, **Legale e Controllo Operativo PNRR** e l'ambito **Supporto Operativo**;

- **Rapporti con la PA, con gli Enti e con gli Utenti**, gestore dell'omonimo macro-processo/funzione, al cui riporto sono articolate l'unità organizzativa **Rapporti con la PA, con gli Enti e con gli Utenti PNRR** e gli ambiti **Promozione Progetti** e **Rapporti con gli Enti e con gli Utenti altri Progetti.**

Alla responsabilità diretta dell'**Amministratore Delegato** sono affidati i seguenti processi (processi di staff),

esternalizzati alla Capogruppo con contratto di **Service**:

- **Risorse Umane;**
- **Affari Legali;**
- **Amministrazione e Bilancio;**
- **Sistemi Informativi;**
- **Supporto Operativo Piattaforma di Gara.**

Alla responsabilità del **Presidente**, cui riportano direttamente gli ambiti "**Gestione service di Capogruppo su Rapporti Istituzionali**" e "**Segreteria**", in accordo con l'A.D., è affidato il processo:

- "**Comunicazione**", parimenti gestito in Service dalla Capogruppo.

Le **unità organizzative** che riportano **al Direttore Generale** (processi di business) corrispondono ai seguenti uffici:

- **Rendicontazione**, gestore dell'omonimo macro-processo, al cui riporto sono articolate le unità organizzative **Rendicontazione MIMIT** e **Rendicontazione e circuito finanziario DTD**;
- **Piano Italia 5G Densificazione,** gestore dell'omonimo macro-processo;
- **Reti Mobili e Connettività,** gestore dell'omonimo macro-processo;
- **Infrastrutture e Operations,** gestore dell'omonimo macro-processo.

Il Direttore Generale è munito di procura conferita dall'Amministratore Delegato.

"**Reti Mobili e Connettività**" e "**Infrastrutture e Operations"** costituiscono le due principali aree di business della Società, e sono organizzate secondo una struttura divisionale al cui vertice sono poste due figure dirigenziali munite di procura, conferita dal Direttore Generale. RMC e INOP a loro volta riportano al D.G.

A "**Reti Mobili e Connettività**" (d'ora in poi anche RMC) riportano le unità organizzative/uffici:

- **Piano Voucher,** gestore dell'omonimo macro-processo;
- **Piano Sanità Connessa** (articolata negli ambiti **lotti 1 e 6, 2 e 4 e 3, 5, 7 e 8**), gestore dell'omonimo macro-processo;
- **Wifi e Servizi Digitali**, gestore dell'omonimo macro-processo;
- **Piano Italia 5GBackhaul,** gestore dell'omonimo macro-processo;
- **Scuole Connesse**, gestore dell'omonimo macro-processo;
- nonché l'ambito **Supporto Operativo**.

A ciascuna unità corrisponde la gestione del processo che porta il nome del Progetto/Piano operativo di riferimento (Voucher, Sanità Connessa, Wifi, 5G, Scuole Connesse).

A "**Infrastrutture e Operations**" (d'ora in poi anche INOP) riportano le unità organizzative/uffici:

- **Gestione Rete** (articolata negli ambiti **Manutenzione, Delivery, Sviluppo**), gestore dell'omonimo macro-processo;
- **Gestione SINFI,** gestore dell'omonimo macro-processo;
- **Business Development,** gestore dell'omonimo macro-processo;
- **Area Operations Nord Est**;
- **Area Operations Nord Ovest**;
- **Area Operations Centro**;
- **Area Operations Sud**;
- **Area Operations Isole**;
- nonché l'ambito **Supporto Operativo**.

Le Business Unit RMC e INOP gestiscono i processi delle "Commesse" affidate in virtù di convenzioni o altri accordi con gli Enti pubblici di riferimento – principalmente, il Ministero delle Imprese e del Made in Italy (MIMIT), Il Dipartimento per la Trasformazione Digitale della Presidenza del Consiglio dei Ministri (DTD), le Regioni – nelle tre modalità di intervento svolte da Infratel Italia, ovvero: modello "a incentivo", nel quale Infratel Italia assume il ruolo di "soggetto attuatore"; modello "concessione", nel quale Infratel Italia, quale ente concedente, assume il ruolo di "stazione appaltante" per la concessione di servizi diretti a costruire, manutenere e gestire dal punto di vista tecnico/commerciale, sulla base degli obblighi stabiliti nell'atto di concessione, la rete, che rimane di proprietà pubblica; nonché la modalità di "intervento diretto", in cui Infratel Italia realizza le opere affidate mediante appalto diretto ad un operatore economico, in qualità di "stazione appaltante" o "committente".
Parte del business di Infratel è inoltre destinata a incrementarsi con i futuri introiti della cessione dei diritti di sfruttamento delle infrastrutture agli operatori del mercato.
In particolare, RMC gestisce tutte le commesse legate principalmente ai fondi PNRR, mentre le Aree Operations Nord Est, Nord Ovest, Centro, Sud, attuano gli interventi "Concessione" e "Piano Italia 1" Giga (piano a incentivo). L'Area Operations Isole, oltre ai predetti processi "Concessione" e "Piano 1 Giga", attua altresì il piano a "intervento diretto" denominato "Isole Minori".
Alle aree sopra individuate corrispondono i processi mappati nel *risk assessment* e associati alle relative procedure.

I.2.4. RESPONSABILE DEI PROCESSI

I soggetti coinvolti nelle attività sensibili e/o strumentali (d'ora in poi anche responsabili di processo sensibile e/o strumentale) hanno la responsabilità di:
- assicurare che il processo sia svolto in linea con i codici di condotta aziendali, in conformità a quanto stabilito dalla Normativa Aziendale e dalla normativa vigente applicabile, nel rispetto dei principi di trasparenza e tracciabilità;
- garantire che vengano eseguiti, da parte dei singoli soggetti coinvolti nel processo, tutti i controlli sulle attività sottostanti definiti nell'ambito dei protocolli di prevenzione specifici di processo.

Sono stati individuati processi sensibili e/o strumentali le cui attività sono riconducibili significativamente a

ciascuna unità organizzativa, come risultante dalla disposizione organizzativa in vigore[2], configurate quindi come aree a rischio. Per ogni unità e per ogni ambito è stata identificata la linea di riporto nell'allegato C, distinguendo tra funzioni facenti capo all'Amministratore Delegato, al Direttore Generale o al Presidente.

I.2.5. RISK OWNERS E PROCESS OWNERS

All'interno dell'organizzazione sono considerati *risk owner* di primo livello i soggetti a qualunque titolo coinvolti nella gestione del processo sensibile e/o strumentale, in quanto soggetti più prossimi al pericolo da gestire.
I responsabili dell'intero processo assumono il ruolo di *process owners*, o *owner* di processo. Tali soggetti sono generalmente individuati nei responsabili dell'unità organizzativa più coinvolta nel processo da gestire. Il *process owner* è riportato nella matrice delle responsabilità allegata al presente Modello, così come ricavata dalle disposizioni organizzative valide al momento di aggiornamento del Modello. In caso di mutamenti organizzativi prevale in ogni caso il ruolo attribuito dalle normative interne e dalle disposizioni organizzative vigenti. Ai responsabili del processo è affidata l'alimentazione dei flussi periodici verso l'OdV, secondo le cadenze previste nello schema allegato al Modello.
Per quanto attiene le Business Units "Reti Mobili e Connettività" e "Infrastrutture e Operations", data la pluralità, rilevanza e complessità degli interventi, il livello di responsabilità del processo è condiviso tra più *process owners*, corrispondenti con il responsabile di processo della singola unità o area operativa che gestisce il singolo processo operativo, e i *risk owners* di secondo livello, corrispondenti rispettivamente con il Responsabile RMC e il Responsabile INOP, che verificano tutti i processi loro affidati per competenza. Fermi gli obblighi di Alta Sorveglianza in ragione delle deleghe gestorie e delle responsabilità del Datore di Lavoro, l'Amministratore Delegato e il Direttore Generale assumono il ruolo di *risk owners* di secondo livello limitatamente ai processi sensibili e/o meramente strumentali gestiti in prima linea dai responsabili delle funzioni sotto ordinate. Ai fini del presente Modello, l'A.D. è il *risk owner* di secondo livello per i contratti di Service, mentre l'*ownership* di primo livello spetta alla funzione competente della Capogruppo, unitamente al referente interno/titolare del Presidio dei contratti di Service (Affari Generali e Demand Organizzazione). Il Presidente è responsabile insieme all'Amministratore Delegato (che è co-*owner*), del Service Comunicazione, affidato a diretto riporto del primo. Resta altresì fermo l'obbligo di Alta Sorveglianza in capo al Consiglio di Amministrazione (quale organo di vertice del sistema di governo del rischio), che promuove, in virtù del suo ruolo strategico, le azioni correttive necessarie, anche su stimolo degli organismi di controllo di terzo livello (funzione Internal Auditing), degli organi sociali e dell'Organismo di Vigilanza.

I.2.6. SISTEMA DEI CONTROLLI INTERNI E GOVERNANCE

Il sistema di governance della Società vede al suo vertice il Consiglio di Amministrazione, il Collegio Sindacale e il Socio Unico Invitalia SpA. Le attività di revisione dei conti sono affidate ad una società di revisione esterna. Il Presidente ha mandato a vigilare sui controlli interni per attuare le linee di indirizzo della Società.
All'interno dei processi aziendali sono sviluppate, in attuazione delle scelte strategiche e di prevenzione adottate dagli organi di governance, le procedure e le altre normative interne la cui osservanza è sanzionata dal sistema disciplinare richiamato dalla Parte speciale del modello e oggetto di controllo operativo e monitoraggio per mezzo di funzioni specialistiche. Oltre al controllo di linea (affidato ai *risk owners* di primo livello) è previsto un livello di controllo intermedio, affidato al management aziendale con competenze specifiche nella gestione di determinati rischi.
I Controlli all'interno di Infratel Italia sono diffusi, avendo la Società optato di non servirsi di funzioni adibite esclusivamente al monitoraggio e controllo (al di fuori della funzione Internal Auditing, di seguito descritta), considerato altresì il supporto esterno offerto dalla Capogruppo per le attività di *compliance*. Pertanto, in virtù dei ruoli effettivamente attribuiti, i dirigenti ed i responsabili di unità organizzative di supporto gestionale svolgono in maniera parallela taluni compiti tipici del *management* del rischio. Tale livello di controllo è

[2] Cfr. Disposizione organizzativa n. 1 e 2 del 1° luglio 2024 e disposizione n. 3 del 1° settembre 2024

attribuito in primo luogo ai manager del sistema di gestione del rischio (SSL, Ambiente, Qualità), nonché ai soggetti muniti di procure e deleghe, ai responsabili ed ai referenti del sistema anticorruzione (RPCT, referenti del Piano di prevenzione della corruzione e della trasparenza) ed ai responsabili ai sensi della normativa sui contratti pubblici (RUP), in ragione del loro obbligo giuridico di vigilare sul rispetto di normative (antinfortunistiche, ambientali, ecc.) e norme di comportamento interne. Inoltre, la Società ha introdotto la funzione Internal Auditing, la quale, anche in coordinamento con la Direzione Internal Auditing di Capogruppo, propone il piano di audit, verifica e monitora la conformità dell'azione dell'Ente al sistema normativo interno e ai protocolli adottati. Il Presidente è delegato a vigilare sull'attuazione delle linee operative dell'attività aziendale tramite la funzione di Internal Auditing, come da poteri conferitigli dal Consiglio di Amministrazione.
Avuto riguardo a specifiche aree, sono previste, in particolare, le seguenti attribuzioni: Acquisti, Affari Generali e Demand Organizzazione coordina l'aggiornamento alla *compliance* 231, verifica gli assetti organizzativi ed i fabbisogni della Società, definisce i ruoli aziendali, presidia i contratti di Service; a Pianificazione, Gare e Ingegneria (al cui interno è individuato il Responsabile dell'Anagrafe Unica delle Stazioni Appaltanti c.d. RASA), che si avvale dell'unità Legale e Controllo operativo PNRR, è affidata la *compliance* normativa di tutte le attività di commessa legate al PNRR; l'unità Pianificazione, Gare e Ingegneria inoltre assiste i RUP e le *business units* nelle procedure di gara (per il tramite dell'unità Gare e Assistenza RUP), assicura la progettazione tecnica delle stesse, la pianificazione e il monitoraggio dei servizi di ingegneria (unità Ingegneria delle Reti e dei Sistemi); Privacy, Qualità, Sicurezza provvede alla gestione del rischio salute e sicurezza sui luoghi di lavoro, del rischio privacy, e dei rischi qualità e ambiente, anche in ragione delle funzioni delegate dal Datore di Lavoro, tramite idonei *manager* del rischio (al responsabile dell'unità è affidato il ruolo di DPO, di Delegato del Datore di Lavoro *ex* art. 16 TUSL ed è anche delegato per gli aspetti ambientali); a Controllo di Gestione è affidato il monitoraggio dell'andamento economico e della performance aziendale.

I.2.7. INTERNAL AUDITING

La Società è dotata di una funzione Internal Auditing che coopera con la funzione Internal Auditing della Capogruppo. La struttura così composta assicura il c.d. "terzo livello di controllo". L'Organismo di Vigilanza è tenuto a vigilare sul funzionamento e sull'osservanza del Modello 231, Parte Generale e Parte Speciale; a tal fine assicura, anche per il tramite dell' Internal Auditing di Capogruppo, la programmazione e attuazione, da parte di auditor qualificati, indipendenti e in possesso di adeguate conoscenze dei processi e dell'organizzazione della Società, di attività di verifica ispettiva interna finalizzate alla valutazione del rispetto degli elementi di controllo definiti, oggetto di comunicazione al Presidente/Amministratore Delegato, all'Organismo di Vigilanza, al RPCT ed alle funzioni interessate.
In raccordo con la funzione dedicata della Capogruppo, la funzione Internal Auditing interna assicura l'obiettivo di:
- proporre il Piano Audit e assicurare la relativa esecuzione;
- effettuare verifiche di conformità al sistema normativo interno e ai protocolli di controllo adottati;
- effettuare le verifiche ispettive e le indagini amministrative.

Il coordinamento delle attività di revisione del Modello 231, Parte Generale e Parte Speciale, è svolto dall'Ufficio Acquisti, Affari Generali e Demand Organizzazione di Infratel Italia, il quale cura altresì il monitoraggio dello scadenzario dei flussi verso l'OdV, attraverso l'apposita piattaforma informatica. Il principale interlocutore del sistema di controllo interno verso l'OdV è la funzione Internal Auditing che pianifica e cura le attività di monitoraggio e controllo, a riporto del Presidente, come da mandato del Consiglio di Amministrazione. Il responsabile della funzione internal auditing promuove e attua una comunicazione strutturata attraverso flussi bidirezionali di dati con le funzioni interessate e con l'OdV, si avvale di un registro condiviso delle attività critiche e dei rischi mappati, con l'ausilio di strumenti idonei, anche informatici, per l'efficace pianificazione e svolgimento delle attività di audit. Il responsabile della funzione internal auditing concorda degli incontri trimestrali con le funzioni per un allineamento continuo e promuove un monitoraggio più efficace, anche attraverso l'integrazione dei dati.

I.3 ATTIVITA' TRASVERSALI

A monte della mappatura dei processi correlati alle strutture organizzative sopra delineate, sono stati individuati, inoltre, **processi trasversali sensibili e/o strumentali le cui attività significative interessano diffusamente vari soggetti titolati della Società.**
Le Aree a Rischio reato trasversali a più uffici individuate sono:

- Rapporti con la Pubblica Amministrazione
- Rapporti con soggetti privati
- Gestione dei finanziamenti, dei fondi e delle concessioni
- Adempimenti nei confronti delle Autorità di Controllo

In tali casi, il *risk owner* di primo livello coincide con i soggetti titolati in applicazione dello Statuto e del sistema di procure e deleghe, mentre il *risk owner* di secondo livello è l'Amministratore Delegato.

In allegato al presente Modello 231 - Parte Speciale sono declinate, in maggior dettaglio, le risultanze dell'attività di mappatura delle aree/attività a "rischio reato" ai sensi del D.Lgs. 231/01; il dettaglio della mappatura delle aree/attività a "rischio reato" ai sensi della L.190/2012 è riportata altresì nel Piano di Prevenzione della Corruzione e della Trasparenza adottato dalla Società.

Fermo restando l'obbligo in capo a tutti i destinatari del Modello 231 - Parte Speciale, di comunicare tempestivamente all'Organismo di Vigilanza ed al RPCT deroghe, anomalie o atipicità eventualmente riscontrate rispetto alle determinazioni contenute nel Modello 231 - Parte Speciale e tutti i fatti, atti o omissioni che possano incidere sull'osservanza dello stesso, il Responsabile di Processo ha inoltre l'obbligo di:

- informare periodicamente l'Organismo di Vigilanza ed il RPCT in merito all'andamento delle attività aziendali, come puntualmente definito nel presente documento e nell'ambito della Normativa Aziendale di riferimento;
- informare tempestivamente l'Organismo di Vigilanza ed il RPCT qualora si verifichino particolari situazioni rilevanti l'efficacia e l'adeguatezza dei protocolli di prevenzione, nonché qualsiasi violazione del Modello 231, Parte Generale e Parte Speciale/PPCT posto in essere da Infratel Italia.

In ogni caso, i responsabili degli Uffici interessati, con cadenza almeno annuale, comunicano all'OdV e al RPCT le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

In allegato al Modello 231 - Parte Speciale sono riassunti tutti i flussi informativi da inviare all'Organismo di Vigilanza, definiti nel presente documento.

I.4 PRINCIPI GENERALI DI CONTROLLO

Gli elementi di controllo, definiti da Infratel Italia anche sulla base delle indicazioni fornite dalle Linee Guida di Confindustria, nonché dalle *"best practices*" nazionali ed internazionali, si basano sui protocolli generali di prevenzione enunciati nei paragrafi che seguono e che sono quindi applicabili a tutti gli Uffici (o aree o processi o funzioni) per le rispettive attività potenzialmente a rischio per come definite nel paragrafo 3. Essi costituiscono i principi generali di controllo posti a base degli strumenti e delle metodologie utilizzate per strutturare gli elementi specifici di controllo, che sono invece predisposti in relazione a specifiche aree di rischio e che sono implementati nelle procedure organizzative e nella restante normativa aziendale.

I.4.1. NORME COMPORTAMENTALI E CODICI DI CONDOTTA

Infratel Italia assicura l'esistenza e la diffusione di un codice etico aziendale (il "Codice Etico") che descriva regole comportamentali di carattere generale a presidio delle attività svolte. In particolare, è fatto espresso divieto, per tutti i destinatari del Modello 231, Parte Generale e Parte Speciale, di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, tutte le fattispecie di reato richiamate dal D.Lgs. 231/01 e dalla L.190/2012;

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti i quali, sebbene risultino tali da non costituire di per sé reato, possano essere strumentali alla loro realizzazione.

I.4.2. POTERI AUTORIZZATIVI E DI FIRMA

Infratel Italia assicura l'esistenza di un sistema di procure e deleghe:

- coerente con le responsabilità organizzative e gestorie assegnate;

- contenente la specifica assegnazione di poteri e limiti, anche di approvazione delle spese, dei Soggetti titolati ad impegnare la Società nei confronti del committente e di parti terze;

- definito nel rispetto dei principi di elaborazione giurisprudenziale e dei requisiti specifici di legge, laddove rilevanti (ad esempio l'art. 16 del D.Lgs. 81/08 e s.m.i. per il caso delle deleghe in materia di sicurezza sul lavoro).

I.4.3. PROCEDURE E NORME INTERNE

Infratel Italia assicura l'esistenza di regole aziendali, disponibili e conosciute all'interno della Società, idonee a stabilire responsabilità e modalità operative per lo svolgimento delle attività sensibili e l'archiviazione della documentazione rilevante.

La Normativa Aziendale declina ruoli e responsabilità di gestione, coordinamento e controllo delle funzioni aziendali a tutti i livelli, descrivendo, in maniera omogenea, le attività proprie di ciascuna struttura.

I.4.4. SEPARAZIONE DEI COMPITI E GESTIONE DEL CONFLITTO D'INTERESSI

Nell'ambito di ciascun processo aziendale rilevante ai sensi del D. Lgs. 231/01, al fine di garantire indipendenza ed obiettività, **è garantito l'intervento di più soggetti e la separazione delle attività tra coloro che sono incaricati di assumere le decisioni/autorizzare gli atti, eseguire le operazioni stabilite, svolgere sulle stesse gli opportuni controlli previsti dalla legge e dalle procedure del sistema di controllo interno**. Un intero processo aziendale, sensibile ai sensi del D.Lgs. 231/01 e della L.190/2012, non può essere affidato ad un unico soggetto. In questo modo la Società intende minimizzare il rischio che un interesse secondario interferisca, ovvero possa interferire, con la capacità del dipendente o collaboratore di agire in conformità ai suoi doveri e responsabilità che sintetizzano l'interesse primario da realizzare.

A tal proposito, inoltre, **il soggetto che, anche potenzialmente, possa trovarsi in una situazione di conflitto di interesse, quando l'esercizio imparziale e obiettivo delle funzioni è compromesso da motivi familiari, affettivi, da affinità politica o nazionale, da interesse economico o da qualsiasi altro interesse personale, diretto o indiretto, ha l'obbligo di astenersi** dal partecipare all'adozione di **decisioni** o ad **attività** che possano coinvolgere alternativamente:

- interessi propri;
- interessi del coniuge, di conviventi, di parenti, di affini entro il sesto grado;
- interessi di persone con le quali abbia rapporti di frequentazione abituale.

Il soggetto si astiene comunque in ogni altro caso in cui esistano gravi **ragioni di convenienza/opportunità**. Sul soggetto grava, oltre all'**obbligo** di astenersi dal votare/decidere/formulare parere, anche quello **di allontanarsi** perché la sola presenza dello stesso può potenzialmente influire sulla libera manifestazione di volontà degli altri membri[3].
Il soggetto è tenuto altresì a rilasciare le dichiarazioni di inconferibilità e incompatibilità previste dalla legge o dai regolamenti interni.

Di tale condizione di conflitto di interesse i destinatari del Modello 231 sono tenuti a dare immediata comunicazione per iscritto al proprio superiore gerarchico o all'organo aziendale competente, il quale valuta, anche con il supporto delle funzioni aziendali a ciò preposte, l'effettiva sussistenza del conflitto e comunica all'Amministratore Delegato, all'Organismo di Vigilanza ed al RPCT le iniziative assunte per rimuoverne gli effetti.

I componenti del vertice amministrativo e degli organi di controllo sociale sono tenuti a dichiarare il conflitto di interessi, rimettendo le decisioni conseguenti al CdA e ai rispettivi organi collegiali di appartenenza. L'Organismo di Vigilanza, anche tramite il Presidente e l'Amministratore Delegato, informa il Collegio Sindacale e il Consiglio di Amministrazione, per provvedere alla nomina di un legale rappresentante legale *ad hoc*, per il caso di conflitto di interessi tra l'Amministratore e l'ente coinvolto in un procedimento 231, per fatto a questi ascritto, nonché degli altri provvedimenti che risultino necessari[4].

Infratel si è dotata di un Regolamento sulla Gestione dei conflitti di interessi cui si fa espresso rinvio per ogni ulteriore elemento di dettaglio.

[3] Il conflitto può riguardare interessi di qualsiasi natura, anche non patrimoniali, come quelli derivanti dall'intento di voler assecondare pressioni politiche, sindacali o dei superiori gerarchici

[4] In caso di conflitto di interesse del Presidente del Consiglio di Amministrazione, del Collegio Sindacale, dell'Organismo di Vigilanza, la comunicazione è rivolta agli altri componenti, su iniziativa di chiunque di essi. Si veda altresì l'art. 39 del D.Lgs. 231/2001.

I.4.5. DIVIETO DI PANTOUFLAGE.

La Legge n. 190/2012 ha introdotto il c.d. divieto di *pantouflage* al comma 16-ter dell'art. 53 D.Lgs. n. 165/2001, volto a contenere il rischio di accordi corruttivi o, comunque, di comportamenti impropri sia del dipendente pubblico, che, facendo leva sulla funzione e sul ruolo ricoperti nella pubblica amministrazione, potrebbe precostituirsi situazioni lavorative vantaggiose presso i privati con cui entra in contatto, sia dello stesso soggetto privato, che di contro potrebbe esercitare pressioni o condizionamenti sul soggetto pubblico, prospettandogli opportunità lavorative o professionali una volta cessato dal servizio, al fine di volgere a proprio favore le scelte dell'amministrazione di appartenenza.
La limitazione all'autonomia negoziale si sostanzia nel divieto per il dipendente pubblico di svolgere, per i tre anni successivi alla cessazione del rapporto di lavoro (qualunque ne sia la causa), attività lavorativa o professionale (di carattere subordinato o autonomo) presso i privati che siano stati destinatari dell'attività dell'amministrazione svolta dal dipendente pubblico medesimo, nel triennio di servizio precedente, con l'esercizio di poteri autoritativi o negoziali per conto dell'amministrazione stessa, e che abbia comportato un vantaggio o un'utilità per i privati in questione (i.e. autorizzazioni, concessioni, sovvenzioni, sussidi e vantaggi economici di qualsiasi genere). Il Piano Anticorruzione adottato dal Infratel Italia S.p.A. ed allegato al Modello, dettaglia le specifiche misure previste dall'Ente.

I.4.6. DOCUMENTABILITÀ E TRACCIABILITÀ

Infratel Italia assicura l'esistenza di regole aziendali, disponibili e conosciute all'interno della Società, idonee a stabilire responsabilità e modalità operative per lo svolgimento delle attività sensibili e l'archiviazione della documentazione rilevante. La Normativa Aziendale declina ruoli e responsabilità di gestione, coordinamento e controllo delle funzioni aziendali a tutti i livelli, descrivendo, in maniera omogenea, le attività proprie di ciascuna struttura.

Il **processo** di decisione, autorizzazione e svolgimento di ciascuna attività sensibile deve essere ricostruibile e **verificabile "ex post"**, attraverso appositi supporti documentali o informatici. Ciascuna operazione/attività relativa ad ogni processo rilevante deve essere adeguatamente documentata. **I documenti rilevanti sono opportunamente formalizzati**, riportano la data di compilazione e la firma del compilatore/sottoscrittore; **gli stessi sono archiviati in luoghi idonei alla conservazione, a cura della funzione competente e con modalità tali da non permettere la modifica successiva se non con apposita evidenza, anche al fine di tutelare la riservatezza dei dati in essi contenuti e di evitare deterioramenti o smarrimenti.**

Qualora sia previsto l'utilizzo di **sistemi informatici** per lo svolgimento delle attività sensibili, gli stessi assicurano:

- la corretta imputazione di ogni singola operazione ai soggetti che ne sono responsabili;
- la tracciabilità di ogni operazione effettuata (inserimento, modifica e cancellazione) dai soli utenti abilitati;
- l'archiviazione e conservazione delle registrazioni prodotte.

La Società provvede, altresì, nel rispetto delle normative vigenti in materia di gestione documentale e gestione informatica del protocollo, a nominare un **Responsabile interno della protocollazione** nonché a definire **opportuna normativa aziendale (Manuale di Gestione del Protocollo informatico)** atta a regolamentare i processi di acquisizione ed invio della documentazione ufficiale, da e verso l'esterno, le relative modalità di registrazione e archiviazione, anche attraverso specifici sistemi informativi dedicati, nonché le modalità di segnalazione e registrazione di possibili danneggiamenti o smarrimenti occorsi; inoltre in applicazione del Codice dell'Amministrazione Digitale e delle Linee Guida AGiD, provvede a nominare il **Responsabile della**

Conservazione e alla definizione di un apposito **Manuale per la Conservazione dei documenti informatici e la dematerializzazione documentale**. **L'accesso ai documenti archiviati**, previa richiesta alle funzioni competenti, è sempre **consentito solo ai soggetti autorizzati**.

I **documenti di terze parti**, di qualsiasi natura e per qualsiasi finalità, contenenti informazioni di natura riservata e/o confidenziale, anche rilevanti a fini di pratiche di concorrenza sleale o antitrust, utilizzabili per ottenere possibili vantaggi o nell'interesse di Infratel Italia, devono essere **tenuti e conservati dai Responsabili delle funzioni interne interessate previa autorizzazione formale da parte dei Soggetti titolati di tale terza parte**.

I.4.7. MONITORAGGIO

La Società affida alle unità organizzative interessate dai processi sensibili anche dei compiti di monitoraggio e reportistica dei dati, sia per il controllo sul raggiungimento degli obiettivi di *performance* e contrattuali, sia per raccogliere le informazioni necessarie al fine di individuare anomalie rispetto al modello organizzativo, per porre in essere ove necessari gli interventi tempestivi, o comunque al fine di alimentare il flusso informativo verso l'OdV. Il monitoraggio è svolto in maniera diffusa su più livelli organizzativi rispettando, anche in questa attività, il principio di definizione e separazione dei ruoli. Per essere efficaci ed imparziali, i controlli devono essere distribuiti in maniera trasversale, diffondendo la cultura della responsabilità ed evitando eccessivi accentramenti, in maniera compatibile con la specificità delle competenze e dei ruoli rivestiti all'interno dell'Ente. Il monitoraggio è svolto sotto la responsabilità dei *process owner* per quanto di competenza, nonché dalle funzioni controllo di gestione e rendicontazione, nei rispettivi ambiti. L' Internal Auditing svolge in maniera indipendente e autonoma il proprio incarico, in stretta collaborazione con la direzione Internal Auditing di Capogruppo, al fine del monitoraggio di tutte le funzioni. la funzione Internal Auditing riferisce e si coordina con l'OdV per quanto di rilievo ai fini del MOGC 231, anche per la pianificazione ed esecuzione di specifiche attività di controllo.

I.4.8. FORMAZIONE

Un ulteriore pilastro del buon funzionamento del MOGC 231 è la formazione. Oltre ai settori in cui la formazione risulta necessaria in adempimento di particolari disposizioni di legge (es.: salute e sicurezza sui luoghi di lavoro), la Società programma attività formative relative ad ambiti sensibili dell'organizzazione. La formazione è periodica. In aggiunta ai c.d. *welcome training* (destinati ai neoassunti), Infratel Italia organizza, con cadenze prestabilite, specifiche attività formative destinate ad accrescere e migliorare il buon funzionamento del MOGC 231. In particolare, prevede una formazione generale sui principi della responsabilità da reato degli enti e sul funzionamento del MOGC 231 adottato. Prevede inoltre approfondimenti mirati e differenziati - in base agli ambiti di competenza e al livello di responsabilità - sul corretto svolgimento delle attività, sugli specifici meccanismi di controllo (in aderenza alle procedure) e sull'utilizzo di *asset* aziendali che presentano vulnerabilità per la sicurezza o la riservatezza (ad es.: in relazione all'uso degli strumenti informatici). Infratel Italia favorisce lo sviluppo delle competenze specifiche necessarie al buon funzionamento dell'Ente, oltreché nella selezione dei *curricula* al momento dell'assunzione, anche nello svolgimento del rapporto lavorativo con i destinatari del MOGC 231, fornendo direttamente con proprio personale o con risorse esterne, al bisogno, la formazione necessaria per l'approfondimento di specifiche tematiche che presentano complessità sul piano tecnico o normativo (es.: in materia di contratti pubblici, di sicurezza informatica, di ingegneria, di ambiente, ecc.). La formazione interna è affidata alla Capogruppo tramite la funzione in *Service* Risorse Umane, o, al bisogno, è affidata a soggetti esterni con adeguate competenze, seguendo la procedura interna appropriata per l'affidamento e per la selezione, in base alla rilevanza dell'affidamento/contratto. Responsabile della verifica del fabbisogno formativo è l'unità Affari Generali e Demand Organizzazione, ad esclusione della formazione in materia di Salute e Sicurezza sui luoghi di lavoro, di competenza dell'unità Qualità, Privacy e Sicurezza.

I.4.9. GESTIONE DEGLI ASSET AZIENDALI

Infratel Italia assicura correttezza, trasparenza e tracciabilità nella gestione degli *asset* aziendali[5] (automobili, telefonia mobile, beni materiali, strumentazione tecnica, etc.) nel rispetto delle leggi, dei regolamenti e delle normative nazionali ed europee applicabili, nonché delle policies/procedure interne in materia; in particolare, l'Unità Acquisti, Affari Generali e Demand Organizzazione, per il mobilio e le automobili, locate direttamente da Infratel Italia, assicura l'inventariazione degli *asset* di pertinenza di ciascuna funzione aziendale, ovvero l'identificazione univoca laddove applicabile, la registrazione a sistema anche attraverso la gestione di un'anagrafica dedicata, l'identificazione del luogo di stoccaggio/utilizzo/installazione e la funzione assegnataria, responsabile del corretto utilizzo e gestione dell'*asset*.
La corretta e puntuale inventariazione degli *asset* è oggetto di verifica periodica anche da parte della funzione Amministrazione presso la Capogruppo per le attività di pertinenza.
l'Unità Acquisti, Affari Generali e Demand Organizzazione, ovvero le funzioni competenti e/o assegnatarie, assicurano la pianificazione e attuazione di opportune attività di manutenzione anche predisponendo opportuni scadenzari e tenendo traccia di tutte le attività connesse, nonché il costante monitoraggio circa lo stato di integrità e conformità degli *asset* alla legislazione vigente.
Le Funzioni assegnatarie assicurano la registrazione dei soggetti utilizzatori dell'*asset*, opportunamente autorizzati dai Soggetti titolati della Società, nonché gli oneri, i termini e le condizioni/regole di utilizzo, tra cui la durata, le finalità/destinazione e motivazioni per l'utilizzo.
Le Funzioni assegnatarie assicurano inoltre opportune attività di monitoraggio circa il corretto utilizzo degli *asset* da parte dei soggetti utilizzatori, accertando il rispetto delle condizioni di utilizzo prestabilite.
I soggetti utilizzatori assicurano, anche sottoscrivendo opportune informative in merito, il rispetto delle policy/procedure definite e di opportuni codici di condotta per la detenzione, l'utilizzo, la custodia e la conservazione degli *asset* in uso; gli utilizzatori sono tenuti altresì a comunicare alle Funzioni assegnatarie, durante il periodo di utilizzo o in fase di restituzione, eventuali variazioni nei parametri di utilizzo prestabiliti, qualsiasi anomalia/non conformità rilevata o verificatasi in fase di utilizzo, nonché possibili eventi di smarrimento o furto.
È fatto divieto ai soggetti assegnatari/utilizzatori di appropriarsi indebitamente, anche temporaneamente, di asset della Società o di terzi.
È fatto divieto altresì di prestare o donare *asset* a soggetti o terze parti a rischio criminalità organizzata, terrorismo e riciclaggio o al fine di ottenere interessi o vantaggi per la Società o per sé stessi.
l'Unità Acquisti, Affari Generali e Demand Organizzazione, anche in collaborazione con le funzioni competenti, assicura la pianificazione e l'attuazione di controlli a campione volti a verificare la correttezza dell'operato delle funzioni assegnatarie e dei soggetti utilizzatori. In esito ai risultati di tali verifiche, l'Unità Acquisti, Affari Generali e Demand Organizzazione procede alla definizione di eventuali opportune azioni correttive, oggetto di comunicazione all'Amministratore Delegato, all'Organismo di Vigilanza ed al RPCT.
Nel caso in cui siano sottoposti a sequestro *asset* di proprietà di Infratel Italia la Funzione competente, ovvero il soggetto interno, formalmente identificato/incaricato dai Soggetti titolati della Società, a cui è affidata la custodia degli stessi, è tenuto a prendere i dovuti provvedimenti al fine di impedirne l'uso, il danneggiamento o la sottrazione, anche tramite la segregazione dei beni confiscati per mezzo di opportuni dispositivi e l'apposizione di idonea segnaletica.
Le modalità di dismissione degli *asset* aziendali, quali smaltimento o alienazione, donazione o vendita, sono stabilite dall'Amministratore Delegato ovvero dalle funzioni competenti in collaborazione con l'Ufficio Servizi Generali e la funzione Amministrazione presso la Capogruppo, previa autorizzazione dell'Amministratore Delegato.
Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate, l'Ufficio Affari Generali e Demand Organizzazione è tenuto alla comunicazione periodica, su base annuale, all'Organismo di Vigilanza, al RPCT e alla funzione Amministrazione e Bilancio presso la Capogruppo di un'informativa riepilogativa dei furti, smarrimenti e dismissione degli *asset* aziendali anche indicativa

[5] Anche asset messi a disposizione del personale Infratel Italia da parte di soggetti terzi (es. appaltatori), previa opportuna formalizzazione della disponibilità e delle modalità di utilizzo dell'asset nell'ambito dei contratti in essere tra le parti.

dell'inventariazione degli *asset* e dei soggetti assegnatari. La funzione Qualità, Privacy e Sicurezza cura la verifica e l'inventariazione degli *asset* per quanto attiene le dotazioni prescritte in materia di sicurezza e ne valuta l'idoneità, anche avvalendosi di consulenti esterni o altri attori del sistema di gestione, ove occorrendo, per l'uso da parte dei destinatari in relazione agli aspetti di salute e sicurezza sui luoghi di lavoro, di trattamento dei dati personali e per gli aspetti ambientali. L'Ufficio Sistemi Informativi presso la Capogruppo e l'Ufficio Gestione Rete, per quanto di rispettiva competenza, sono tenuti a una comunicazione periodica, in coordinamento con l'Ufficio Acquisti, Affari Generali e Demand Organizzazione, su base annuale, all'Organismo di Vigilanza, al RPCT e alla funzione Amministrazione e Bilancio presso la Capogruppo di un'informativa riepilogativa dei furti, smarrimenti e dismissione degli *asset* aziendali anche indicativa dell'inventariazione degli *asset* e dei soggetti assegnatari.
Inoltre, in funzione della gravità dell'evento accaduto, valutano se effettuare una comunicazione tempestiva all'OdV. Le sopra dette funzioni comunicano tempestivamente all'OdV anomalie nella gestione dei beni aziendali eventualmente posti sotto sequestro per finalità amministrative o giudiziarie.

In ogni caso, i responsabili degli Uffici interessati, con cadenza almeno annuale, comunicano all'OdV e al RPCT le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

I.4.10. GESTIONE DELLE INFORMAZIONI RISERVATE

Le informazioni sono una componente essenziale del patrimonio aziendale.
Informazioni, dati e conoscenze acquisite, elaborate e gestite dai dipendenti/collaboratori di Infratel Italia nell'esercizio dell'attività lavorativa devono rimanere strettamente riservate e opportunamente protette e non possono essere utilizzate, comunicate o divulgate se non nel pieno rispetto della normativa vigente e degli elementi di controllo a seguire riportati.

L'**Amministratore Delegato**, avvalendosi della collaborazione delle funzioni competenti, assicura, nel rispetto delle disposizioni normative vigenti:

- la predisposizione di un disciplinare interno contenente l'indicazione della tipologia e della natura delle informazioni aziendali che debbono rimanere riservate, nonché le responsabilità e le modalità di utilizzo verso l'interno e l'esterno della Società;

- la sottoscrizione, da parte del personale interessato, interno ed esterno, di un atto di impegno al rispetto della riservatezza delle informazioni identificate in detto disciplinare;

- fermi restando la trasparenza delle attività poste in essere e gli obblighi di informazione imposti dalle disposizioni vigenti, è obbligo del personale assicurare la riservatezza richiesta dalle circostanze per ciascuna notizia appresa in ragione della propria funzione lavorativa, anche al fine di minimizzare il rischio del reato ex L.190/12 di "Rilevazione e utilizzazione di segreti di ufficio".

- È assicurata, altresì, in aderenza alle procedure e alle istruzioni operative di Gruppo, la gestione delle informazioni privilegiate, ossia di quelle informazioni rilevanti ai sensi dell'art. 180 TUF (informazioni c.d. price sensitive). Tali informazioni vanno trattate con correttezza e secondo livelli adeguati di autorizzazione. Laddove il destinatario del MOGC 231 venga a conoscenza di tali informazioni è fatto assoluto divieto di utilizzare le informazioni apprese per scopi personali e di rivelarle a soggetti non autorizzati o comunque, anche quando autorizzati, all'infuori dei propri compiti e obblighi di fedeltà verso l'ente.

Nessun dipendente/collaboratore di Infratel Italia può trarre vantaggi di alcun genere, diretti o indiretti, personali o patrimoniali, **dall'utilizzo di informazioni riservate**, né comunicare dette informazioni ad altri o raccomandare o indurre altri all'utilizzo delle stesse. **La comunicazione a terzi** delle informazioni riservate deve avvenire **esclusivamente da parte di Soggetti autorizzati** ed in ogni caso in conformità alle disposizioni aziendali ed al suddetto disciplinare, al Piano di Prevenzione della Corruzione e della Trasparenza e ai regolamenti e alle IO della Capogruppo sulla gestione delle informazioni privilegiate.

L'unità Affari Generali, Acquisti e Demand Organizzazione e l'unità Pianificazione, Gare e Ingegneria, anche avvalendosi della collaborazione della funzione Affari Legali di Capogruppo, nell'ambito dell'attività di competenza relativa alla redazione degli **atti/contratti con parti terze**, assicurano la definizione di specifiche **clausole di risoluzione e salvaguardia relative al mantenimento della confidenzialità di eventuali informazioni riservate/rilevanti**.
Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate, tutti i soggetti destinatari del Modello, gli Amministratori, i Responsabili di Ufficio/funzione sono tenuti a comunicare tempestivamente al RPCT ogni eventuale rivelazione di notizia che debba rimanere segreta/riservata di cui venga a conoscenza nell'esercizio delle proprie attività.

La Società adotta le cautele necessarie per rispettare la riservatezza delle comunicazioni ed impedire atti fraudolenti sugli *asset* aziendali utilizzati per le comunicazioni con l'interno e con l'esterno. Inoltre, la Società distingue i livelli di autorizzazione per l'accesso alle informazioni, sia in fase di gestione del dato, che di controllo. Si rinvia a quanto descritto nel paragrafo precedente, nonché nel capitolo delle misure specifiche previste per

l'ambito *Privacy* e per la gestione dei sistemi informativi.

In ogni caso, i responsabili degli Uffici interessati, con cadenza almeno annuale, comunicano all'OdV e al RPCT le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance)

I.4.11. MODELLO ORGANIZZATIVO EX D.LGS. N.231/01 E SISTEMA DI GESTIONE DELLA SALUTE E SICUREZZA SUI LUOGHI DI LAVORO EX ART. 30 D.LGS. 81/2008 (TU SICUREZZA LAVORO)

Infratel Italia ha adottato e certificato il sistema di gestione della sicurezza sul lavoro, conforme ai requisiti di cui all'art. 30 del D.Lgs. 81/08 e s.m.i. e della UNI ISO 45001:2018; nell'ambito di applicazione di tale sistema ha identificato e nominato - quindi reso noto all'interno dell'organizzazione - il rappresentante della Direzione (RDD) per la Sicurezza, a cui sono state assegnate specifiche responsabilità:

- garantire che il sistema di gestione della salute e sicurezza sul lavoro sia definito, attuato e mantenuto attivo in accordo agli standard di riferimento (art. 30 D.Lgs. 81/08 e UNI ISO 45001:2018);
- garantire che le informazioni/registrazioni relative alle prestazioni del sistema di gestione siano presentate ai vertici aziendali per il riesame ed utilizzate come base per il miglioramento.

I due sistemi di gestione (MOGC 231 e SSL) si integrano a vicenda, costituendo il primo lo strumento attraverso cui la Società rende efficace il sistema di gestione SSL, attraverso l'individuazione dei soggetti responsabili e la predisposizione di specifici elementi di controllo, organizzativi e disciplinari, che ne presidiano l'osservanza e la corretta funzionalità.

Allo stesso tempo, il SGSSL costituisce il sottosistema attraverso cui la Società individua, valuta e gestisce efficacemente i rischi di infortuni e malattie professionali, attraverso la pianificazione, l'attuazione, l'esecuzione, la verifica e il riesame delle azioni e dei presidi a tutela della salute e sicurezza sui luoghi di lavoro.

Infratel Italia individua all'interno della propria organizzazione **specifiche figure responsabili della pianificazione, gestione e monitoraggio delle attività legate alla salvaguardia della sicurezza e della salute sui luoghi di lavoro**. L'elenco delle suddette figure comprende:

- **Datore di lavoro**, responsabile della definizione della politica aziendale in merito alla salute e alla sicurezza sui luoghi di lavoro, nonché della valutazione dei rischi e della nomina del RSPP;
- **Delegato del datore di lavoro:** il Datore di lavoro, ai sensi della normativa vigente, previa verifica del possesso di adeguati requisiti professionali e di esperienza, individua un suo delegato per tutte le attività tranne per quelle definite nell'art. 17 D.Lgs. 81/08;
- **Incaricati per la sicurezza/Responsabile del sistema di gestione**: il Datore di lavoro, ai sensi della normativa vigente[6], previa verifica del possesso di adeguati requisiti professionali e di esperienza, incarica dei soggetti interni quali referenti per la gestione di specifici aspetti di sicurezza, in coerenza con l'ambito di competenza della funzione aziendale da essi ricoperta. Nello specifico, le figure degli Incaricati per la sicurezza assumono il ruolo di: Referente per la sicurezza generale; Referente per la sicurezza nei cantieri; Responsabile del sistema di gestione della sicurezza, avente il compito di garantire l'attuazione delle attività previste dal sistema di gestione della sicurezza adottato dalla Società;
- **Responsabile del servizio prevenzione e protezione (RSPP),** nominato dal Datore di lavoro dopo aver consultato il Rappresentante dei lavoratori, previa verifica del possesso dei requisiti previsti dalla normativa vigente;
- **Medico Competente (MC),** nominato dal Datore di lavoro;
- **Responsabile dei lavori (RL):** l'Amministratore Delegato rappresenta la Committenza per tutti gli adempimenti di cui all'articolo 90 del D.Lgs. 81/08 e s.m.i., recante *"Obblighi del committente o del responsabile dei lavori"*; pertanto, nell'ambito della gestione dei cantieri temporanei e mobili ai sensi del Titolo IV del D.Lgs.

[6] Art. 16 D.Lgs. 81/08 e s.m.i.

81/08, individua un RL al quale delega gli obblighi di cui al richiamato articolo;

- **Incaricati alle emergenze** per le squadre antincendio e primo soccorso: l'individuazione di tali figure è definita mediante lettera di incarico, previa verifica di assenza di eventuali fattori ostativi, del possesso di specifici requisiti (anche in termini di copertura di turni di lavoro e localizzazione) e dell'avvenuta formazione in accordo alle disposizioni legislative in materia;
- **Rappresentante dei lavoratori per la sicurezza (RLS)**, nominato dai lavoratori, ai sensi della normativa vigente.

Il Datore di lavoro, anche per il tramite del suo delegato, è tenuto a vigilare sull'attività svolta dai suoi incaricati, attraverso la definizione di opportune reportistiche oggetto di comunicazione periodica da parte dei soggetti vigilati.

Tutti i lavoratori sono esposti a pericoli per la salute e la sicurezza sui luoghi di lavoro, che hanno dunque carattere trasversale. I lavoratori sono tenuti, quali attori del sistema di salute e sicurezza sui luoghi di lavoro, a rispettare le cautele imposte dalla legge, dal presente MOGC 231, dalla normativa aziendale e da ogni altra circostanza di fatto, con la dovuta diligenza, per preservare la propria incolumità e quella dei colleghi.

I.4.12. MODELLO ORGANIZZATIVO EX D.LGS. N.231/01 E REGOLAMENTO GENERALE SULLA PROTEZIONE DATI N. 679/2016 (GDPR)

Si rende necessario evidenziare il parallelismo tra gli strumenti di compliance normativa in ambito privacy ex Regolamento Generale sulla Protezione Dati n. 679/2016 (di seguito "GDPR") e i modelli di organizzazione contemplati dagli artt. 6 e 7 del D.Lgs. 231/01, idonei ad escludere la c.d. "colpa organizzativa" in capo all'ente da soggetti che rivestono funzioni apicali o subordinate al suo interno con riferimento alla **prevenzione del rischio della commissione di reati nell'ambito di un trattamento illecito dei dati personali.**

Il modello organizzativo ex D.Lgs. 231/01 non prevede espressamente i reati contro la *privacy* di cui agli artt. 167 e seguenti del D.Lgs. 196/2003 tra quelli in grado di determinare la responsabilità dell'ente. Tuttavia, alcuni illeciti presuppongono un *data breach* ai sensi del GDPR.

In questi casi, le misure organizzative che delineano controlli preventivi in applicazione del D.Lgs. 231/01, al fine di esonerare l'ente dalla responsabilità per reati commessi nel suo interesse e/o a suo vantaggio, sono funzionali a tutelare indirettamente anche i diritti e le libertà dei titolari di dati personali soggetti a trattamento. Da questo punto di vista è dunque possibile considerare integrati i due sistemi.

Ad esempio, i rischi legati alla riservatezza e all'integrità dei dati personali determinato dall'accesso abusivo ad un sistema informatico, oppure all'installazione di *software* (ad esempio il c.d. *trojan*) e di altri programmi in grado di acquisire fraudolentemente comunicazioni informatiche o di danneggiare sistemi operativi costituiscono presupposti dei reati informatici ex artt. 615 ter, 617 *quinquies* e 635 *ter* c.p. che sono considerati "**Delitti informatici e trattamento illecito di dati**" **ex art. 24 bis del D.Lgs.231/01**.
Dunque, in applicazione del D.Lgs. 231/01 tali fattispecie prevedono e puniscono ipotesi rientranti nella disciplina della privacy, a tutela non solo dei dati personali bensì di tutti i dati.

Pertanto, ove sia **carente ovvero non dimostrabile un'adeguata tutela dei dati personali** si configura il rischio di tali ipotesi delittuose.

È quindi necessaria una documentata osservanza tanto della normativa del GDPR quanto del D.Lgs. 231/01 per configurare valida esimente a riguardo.

Il modello di gestione *privacy*, ove adottato, costituisce un sistema di gestione integrato col MOGC 231, per consentire una valutazione più accurata del rischio relativo al trattamento dei dati personali.

A tal proposito si rinvia da un lato agli **obblighi previsti dall'art. 24 del GDPR**, in capo al titolare del trattamento, di mettere in atto le misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento e dall'altro **all'onere in capo all'ente previsto dall'art. 6 c.1 let. A del D.Lgs. 231/01** di adottare ed attuare efficacemente un modello di organizzazione idoneo a prevenire la commissione dei reati, la cui prova esonera l'ente dalla responsabilità per il reato commesso.

L'osservanza delle regole a tutela del corretto trattamento dei dati - in particolare per quanto riguarda l'uso degli strumenti informatici - è un obbligo trasversale per tutti i destinatari del modello. Essi devono rispettare la normativa aziendale a tutela della propria ed altrui riservatezza, in relazione ad ogni attività compiuta nell'interesse o a vantaggio dell'Ente.

I.4.13. MODELLO ORGANIZZATIVO EX D.LGS. N.231/01 E PIANO DI PREVENZIONE DELLA CORRUZIONE E DELLA TRASPARENZA (L. 190/2012)

Infratel Italia, quale Società "in house" del MIMIT, in ragione del controllo diretto ed indiretto esercitato dalla PA, ha nominato **il Responsabile della Prevenzione della Corruzione e della Trasparenza, e adottato il relativo Piano di Prevenzione.**

Congiuntamente al Piano, il Modello risulta rafforzato dall'inclusione dei delitti contro la Pubblica amministrazione rilevanti *ex* L. 190/2012, facendo sì che il MOGC 231 risulti esteso in funzione di prevenzione dei delitti contro la P.A. esclusi dal D.Lgs. 231/2001, ed in particolare delle fattispecie a danno degli interessi e del prestigio dell'amministrazione di cui agli **artt. 314** (peculato), **314-bis** (indebita destinazione di denaro o cose mobili) **e 316** (peculato mediante profitto dell'errore altrui)**,** anche al di fuori delle ipotesi di consumazione dell'illecito in danno degli interessi finanziari dell'Unione europea, **gli artt. 326 (rivelazione o utilizzazione di segreto d'ufficio), 328** (omissione o rifiuto di atti di ufficio), **334** (sottrazione o danneggiamento di cose sottoposte a sequestro disposto nel corso di un procedimento penale o dall'autorità amministrativa), **335** (violazione colposa di doveri inerenti alla custodia di cose sottoposte a sequestro disposto nel corso di un procedimento penale o dall'autorità amministrativa) **c.p.**

Il Piano di Prevenzione della Corruzione e della Trasparenza, secondo la logica dei sistemi integrati finora analizzata, in coordinamento col MOGC 231, contribuisce pertanto ad una valutazione più accurata del rischio di reati contro la Pubblica amministrazione, per la prevenzione delle condotte satellite e degli altri comportamenti sintomatici o prodromici degli eventi corruttivi, la cui prevenzione, anche se estranei al D.lgs. 231/2001, in attuazione del PPCT, rientra tra gli scopi del Modello.

I.4.14. MODELLO ORGANIZZATIVO E DISCIPLINA SUL WHISTLEBLOWING (D.LGS. 24/2023).

La Società ha adottato, in conformità alle disposizioni di cui al D.Lgs. 24/2023 (decreto attuativo della Direttiva 2019/1937 UE del Parlamento europeo e del Consiglio), una piattaforma di segnalazione degli illeciti (c.d. *whistleblowing*) modellata secondo gli indirizzi euro-unitari e secondo le linee guida fornite dall'ANAC. La piattaforma garantisce la riservatezza del segnalante, secondo gli *standard* tecnici imposti dalla legge ed è altresì prevista la tutela dalle ritorsioni in caso di segnalazioni, sia all'interno del MOGC 231, che all'interno della procedura di gestione delle segnalazioni di violazioni e illeciti.

La piattaforma è gestita dal Responsabile della Prevenzione della Corruzione e della Trasparenza ed è utilizzabile per segnalazioni di rilievo più ampio rispetto alla disciplina *ex* D.Lgs. 231 del 2001, anche relativamente a questioni estranee al campo di applicazione del MOGC 231. La piattaforma è unificata e costituisce uno dei canali di comunicazione, in conformità alle previsioni dell'art.6, comma 2-bis, d.lgs. 231/2001. Di conseguenza,

il gestore del sistema di *whistleblowing* (c.d. *whistleblowing officer*, individuato nel RPCT) è responsabile di informare l'OdV delle segnalazioni ricevute, ove queste siano rilevanti rispetto al Modello. Qualora la segnalazione riguardi direttamente il Responsabile della Prevenzione della Corruzione e della Trasparenza, o nel caso in cui questo si trovi una situazione di conflitto di interessi, la comunicazione sarà indirizzata all'OdV di Infratel Italia selezionando il destinatario attraverso la piattaforma stessa, oppure con i canali alternativi di contatto relativi a questo.

La legittimazione alla presentazione di segnalazioni in qualità di "whistleblower" è ampliata rispetto ai destinatari del MOGC e comprende, oltre ai dipendenti, anche tutti quei soggetti collegati in senso ampio all'organizzazione nella quale si è verificata la violazione e che potrebbero temere ritorsioni. Possono presentare segnalazioni, infatti: il personale interno della Società; i lavoratori autonomi, collaboratori, liberi professionisti e consulenti che svolgono la propria attività lavorativa per Infratel Italia; i dipendenti e i collaboratori dei fornitori di lavori, beni e servizi da essa commissionati; i volontari e i tirocinanti (anche non retribuiti); gli azionisti e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza della Società, anche qualora tali funzioni siano esercitate in via di mero fatto.

I.4.15. MODELLO ORGANIZZATIVO E SISTEMA DI GESTIONE INTEGRATO QUALITÀ E AMBIENTE.

Il Modello organizzativo va coordinato altresì con il sistema di Gestione Integrato Qualità e Ambiente, atteso che la Società adotta un unico *set* di procedure e di altre normative interne, che devono al contempo conformarsi tanto con il MOGC 231, quanto con gli altri modelli di gestione interni.
In particolare, il SGIQA contribuisce ad una valutazione più accurata dei rischi per la qualità e per l'ambiente. Il Responsabile del Sistema di Gestione Integrata del Rischio Qualità e Ambiente (RSGIQA) verifica le procedure adottate in conformità del Modello. La funzione responsabile del coordinamento delle attività 231 comunica tempestivamente all'OdV l'elenco delle procedure modificate al momento della loro approvazione, nonché l'elenco di quelle di nuova introduzione, con l'indicazione dei rispettivi ambiti. Il RSGIQA comunica le non conformità rilevanti e l'AD, di concerto con le funzioni interessate, procede alle opportune azioni correttive. L'Amministratore delegato, all'esito della procedura di riesame, comunica tempestivamente all'OdV le eventuali criticità riscontrate rilevanti per il MOGC 231.

CAPITOLO II GESTIONE TRASVERSALE DEI RAPPORTI CON SOGGETTI ESTERNI

II.1 PROCESSI TRASVERSALI

In questo paragrafo sono trattate le attività sensibili e/o strumentali che, per loro natura, interessano diffusamente il personale di Infratel Italia all'interno di più processi. Si tratta dei rapporti economici ed istituzionali con i soggetti esterni, pubblici e privati, delle attività di gestione di fondi, beni e finanziamenti pubblici e dei rapporti con le Autorità di controllo pubblico.

In tali casi, il Responsabile di processo di secondo livello coincide con la figura dell'Amministratore Delegato, mentre i responsabili di primo livello coincidono con i Soggetti titolati di Infratel Italia a svolgere le attività per conto dell'Ente, sulla base del sistema di procure e deleghe in vigore. I processi trasversali sensibili e/o strumentali individuati sono:

- Gestione dei rapporti con i soggetti pubblici (PA centrale, Regioni, Enti locali, A.G., articolazioni territoriali, Autorità di controllo nazionali e sovranazionali, altri soggetti pubblici committenti);
- Gestione dei rapporti con i soggetti privati (imprese, utenti, soci, creditori, cittadini);
- Gestione dei finanziamenti (sia in relazione alla richiesta che all'erogazione degli stessi) e delle concessioni;
- Gestione degli adempimenti nei confronti delle autorità pubbliche e degli organi di controllo.

Gli elementi di controlli legati ai suddetti processi trasversali, enunciati di seguito, si applicano a tutti gli Uffici aziendali coinvolti.

II.1.1. GESTIONE DEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Gestione rapporti con P.A. centrale (MIMIT - DTD, ADE, altre amministrazioni centrali);	Pres./A.D./D.G./Procuratore RMC/Procuratore IO/Delegato/ Resp. rendicontazione/altri soggetti legittimati	Peculato, peculato d'uso ed indebita destinazione quando commessi ai danni dell'UE; corruzione attiva e passiva, concussione, induzione indebita a dare o promettere denaro o altra utilità nei rapporti tra soggetti di INF e soggetti del MIMIT, del DTD, dell'ADE o altre amministrazioni centrali; istigazione alla corruzione; traffico di influenze illecite; malversazione di fondi pubblici; percezione indebita di erogazione; truffe ai danni di PA centrali e locali; falsità in documento pubblico informatico; reati tributari	**RISCHIO DIRETTO:** **Art. 25 d.lgs. 231/2001 (artt. 314, 314-bis, 316, 317, 318, 319, 319-quater, 321, 321, 322, 346-bis c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs. 231/2001 (artt. 316-bis, 316-ter, 640, 640-bis c.p.);** **Art. 24-bis d.lgs 231/2001 (art. 491-bis c.p.);** **Art. 25-quinquiesdecies d.lgs. 231/2001 (artt. 2, 3, 8, 10, 11 d.lgs 74/2000)**
Gestione rapporti con articolazioni territoriali della P.A.;	A.D./D.G./Procuratore RMC/Procuratore IO/Delegato/altri soggetti legittimati	Peculato, peculato d'uso ed indebita destinazione quando commessi ai danni dell'UE; corruzione attiva e passiva; concussione; induzione indebita a dare o promettere denaro o altra utilità nei rapporti appartenenti a Pubbliche Amministrazioni decentrate; istigazione alla corruzione; traffico di influenze illecite; malversazione di fondi pubblici; percezione indebita di erogazione; truffe ai danni di PA centrali e locali; falsità in documento pubblico informatico	**RISCHIO DIRETTO:** **Art. 25 d.lgs. 231/2001 (artt. 314, 314-bis, 316, 317, 318, 319, 319-quater, 321, 321, 322, 346-bis c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs. 231/2001 (artt. 316-bis, 316-ter, 640, 640-bis c.p.);** **Art. 24-bis d.lgs 231/2001 (art. 491-bis c.p.)**

Gestione rapporti con Regioni ed Enti Locali	A.D./D.G./Procuratore RMC/Procuratore IO/Delegato/altri soggetti legittimati	Peculato, peculato d'uso ed indebita destinazione quando commessi ai danni dell'UE; corruzione attiva e passiva; concussione; induzione indebita a dare o promettere denaro o altra utilità nei rapporti appartenenti Enti Locali; istigazione alla corruzione; traffico di influenze illecite; malversazione di fondi pubblici; percezione indebita di erogazione; truffe ai danni di PA centrali e locali; traffico di influenze illecite; falsità in documento pubblico informatico	**RISCHIO DIRETTO:** **Art. 25 d.lgs. 231/2001 (artt. 314, 314-bis, 316, 317, 318, 319, 319-quater, 321, 321, 322, 346-bis c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs. 231/2001 (artt. 316-bis, 316-ter, 640, 640-bis c.p.);** **Art. 24-bis d.lgs 231/2001 (art. 491-bis c.p.)**
Gestione rapporti con Autorità di controllo nazionali	Pres./A.D./D.G./Procuratore RMC/Procuratore IO/Delegato/Resp. rendicontazione/altri soggetti legittimati	Peculato, peculato d'uso ed indebita destinazione quando commessi ai danni dell'UE; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere denaro o altra utilità nei rapporti appartenenti a Autorità di controllo o vigilanza; istigazione alla corruzione; traffico di influenze illecite; malversazione di fondi pubblici; percezione indebita di erogazione; truffe ai danni di PA centrali e locali	**RISCHIO DIRETTO:** **Art. 25 d.lgs. 231/2001 (artt. 314, 314-bis, 316, 317, 318, 319, 319-quater, 321, 321, 322, 346-bis c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs. 231/2001 (artt. 316-bis, 316-ter, 640, 640-bis c.p.)**
Gestione rapporti con Autorità di controllo europee	Pres./A.D./D.G./Procuratore RMC/Procuratore IO/Delegato/Resp. rendicontazione/altri soggetti legittimati	Peculato, peculato d'uso ed indebita destinazione quando commessi ai danni dell'UE; corruzione attiva e passiva; concussione; induzione indebita a dare o promettere utilità, corruzione attiva e passiva, corruzione in atti giudiziari, istigazione alla corruzione - di membri degli organi UE o di funzionari UE; traffico di influenze illecite	**RISCHIO DIRETTO:** **Art. 25 d.lgs. 231/2001 (artt. 314, 314-bis, 316, 322-bis, 346-bis c.p.)**
Gestione rapporti con A.G.	Presidente/AD/Delegato/Legale	Corruzione attiva di appartenenti all'autorità giudiziaria; induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria	**RISCHIO DIRETTO:** **Art. 25 d.lgs. 231/2001 (art. 319-ter c.p.);** **Art. 25 decies d.lgs. 231/2001 (art. 377-bis c.p.)**
Conclusione di contratti/accordi/convenzioni e affidamenti con soggetti pubblici committenti	A.D./D.G./Procuratore RMC/Procuratore IO/Delegato/altri soggetti legittimati	Peculato, peculato d'uso ed indebita destinazione quando commessi ai danni dell'UE; corruzione attiva e passiva; concussione; induzione indebita a dare o promettere denaro o altra utilità; istigazione alla corruzione; traffico di influenze illecite; truffe, anche informatiche, ai danni di PA centrali e locali; turbata libertà degli incanti o del procedimento di scelta del contraente, truffe, anche informatiche, ai danni di PA centrali o locali; falsità in documento pubblico informatico; malversazione e indebita percezioni di fondi pubblici; frode nelle pubbliche forniture	**RISCHIO DIRETTO:** **Art. 25 d.lgs. 231/2001 (artt. 314, 314-bis, 316, 317, 318, 319, 319-quater, 321, 321, 322, 346-bis c.p.);** **Art. 24 d.lgs. 231/2001 (artt. 353, 353 bis,** **640, 640-bis, 640-ter c.p.);** **Art. 24-bis d.lgs 231/2001 (art. 491-bis c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs. 231/2001** **(artt. 316-bis, 316-ter, 356 c.p.)**

II.1.2. ELEMENTI DI CONTROLLO DELLA GESTIONE DEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

II.1.2.1. Gestione dei rapporti istituzionali o economici con soggetti appartenenti alla Pubblica Amministrazione, con le Autorità indipendenti di controllo e vigilanza, con le Autorità europee.

Per conto di Infratel Italia, possono intrattenere rapporti con la Pubblica Amministrazione, con la sola eccezione delle attività tecniche ed operative preordinate all'esecuzione delle convezioni/contratti/programmi in essere,

i soggetti (dipendenti, membri degli organi sociali, collaboratori esterni, consulenti o partner) a cui sia stato formalmente conferito incarico in tal senso (con apposita procura o disposizione organizzativa per i soggetti interni, ovvero con apposita clausola nel contratto di collaborazione o consulenza o partnership per gli altri soggetti indicati).
Gli incontri con i rappresentanti del committente o con soggetti pubblici quali meeting di natura decisionale o programmatica, strumentali o finalizzati alla formalizzazione di atti/contratti/convenzioni ovvero alla richiesta di finanziamenti/contributi/agevolazioni oppure legati a Stati Avanzamento Lavori prodromici al processo di rendicontazione verso il committente o comunque legati all'accettazione della prestazione o servizio erogati dalla Società, devono essere presenziati preferibilmente da due rappresentanti di Infratel Italia. Di detti incontri deve comunque essere redatto apposito verbale. Tali informazioni devono essere comunicate al proprio responsabile e al RPCT[7], quindi archiviate e conservate.

Gli incontri devono essere condotti nel rispetto del Codice Etico e, in particolare, in ottemperanza alle seguenti prescrizioni:

- non è consentito a coloro che operano per conto di Infratel Italia, direttamente o indirettamente, né per il tramite di interposta persona, realizzare attività, sotto qualsiasi forma, che abbiano come effetto l'illecito condizionamento di soggetti pubblici; pertanto, non è consentito offrire o promettere denaro, doni, compensi o altra utilità, sotto qualsiasi forma, né esercitare illecite pressioni o promettere qualsiasi oggetto, servizio, prestazione, o favore a dirigenti, funzionari o dipendenti della Pubblica Amministrazione, ovvero incaricati di pubblico servizio, o a loro parenti, conviventi, anche per il tramite di interposta persona, allo scopo di influenzare il giudizio nell'ambito di qualsiasi tipologia di rapporto con gli stessi instaurato;
- non è altresì consentito a coloro che operano per conto di Infratel Italia, direttamente o indirettamente, né per il tramite di interposta persona, ricevere denaro, doni, favori, compensi o utilità, sotto qualsiasi forma, che possano influenzare il proprio giudizio nell'ambito di qualsiasi tipologia di rapporto con soggetti terzi rilevanti quali, a titolo indicativo, committente, beneficiari e fornitori;
- è fatto obbligo di instaurare e gestire qualsiasi rapporto con la Pubblica Amministrazione sulla base di criteri di massima correttezza, imparzialità, trasparenza e buona fede;
- non è consentito utilizzare o presentare dichiarazioni e documenti attestanti fatti e notizie non vere, ovvero omettere informazioni per conseguire l'aggiudicazione di un contratto/convenzione/finanziamento/erogazione o l'approvazione di un rapporto rendicontativo, nonché qualsiasi attività/operazione/atto a vantaggio o nell'interesse di Infratel Italia.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate, chiunque riceva richieste esplicite o implicite di benefici di qualsiasi natura da parte di dirigenti, funzionari o dipendenti della Pubblica Amministrazione, o che sia indotto dagli stessi a dare o promettere denaro o altre utilità anche a soggetti terzi, è tenuto ad informare tempestivamente l'OdV ed il RPCT, quindi a sospendere immediatamente ogni rapporto con essi.

II.1.2.2. Contratti/accordi/convenzioni e affidamenti con soggetti pubblici committenti

L'individuazione delle opportunità di business di Infratel Italia ed il successivo sviluppo sono coerenti con la mission aziendale e con gli obiettivi strategici definiti dal Consiglio di Amministrazione.

Le attività di *scouting*, finalizzate all'individuazione di possibili nuovi progetti, ovvero le attività di negoziazione con il committente, finalizzate alla definizione dei contenuti e degli aspetti tecnici, operativi ed economici degli accordi/convenzioni, sono condotte dall' Amministratore Delegato, in collaborazione con le funzioni interne

[7] Secondo le tempistiche dallo stesso definite. Le motivazioni di eventuali deroghe alla predisposizione della sintesi degli incontri sono oggetto di comunicazione tempestiva al RPCT.

preposte e competenti, nel rispetto dei codici di condotta e dei protocolli di gestione relativi al rapporto con soggetti della Pubblica Amministrazione. L'esito di dette attività è opportunamente formalizzato in una relazione contenente le caratteristiche tecnico/economiche del rapporto.

I contratti/convenzioni che la Società stipula con i propri committenti sono sottoposti a validazione e firma da parte dell'Amministratore Delegato e/o rimessi all'approvazione del CDA in base al sistema di procure/deleghe in essere[8].
A ciascun contratto/convenzione è associato, ove previsto, un Disciplinare di rendicontazione elaborato dal committente in relazione alle fonti di finanziamento del progetto e un Piano delle attività che viene comunicato in via ufficiale al committente dai Soggetti titolati della Società. Tale Piano è elaborato da Pianificazione in funzione della tipologia di commessa, quindi verificato ed approvato dall' Amministratore Delegato[9].

Rendicontazione assicura prima dell'avvio del processo di rendicontazione, la corretta interpretazione del Disciplinare di rendicontazione, allegato a ciascuna Convenzione; l'esito di tale attività può richiedere la predisposizione di linee guida operative, a uso interno, per chiarire la portata normativa delle disposizioni del Disciplinare di rendicontazione.

Il Disciplinare è formalmente comunicato da Rendicontazione alle funzioni aziendali interessate.
La predisposizione della documentazione oggetto di scambio con il committente deve essere effettuata con la massima diligenza e professionalità in modo da fornire informazioni chiare, accurate, complete, fedeli e veritiere evitando e comunque segnalando, nella forma e nei modi idonei, eventuali situazioni di conflitto di interesse;

Ai fini del corretto e legittimo accesso ai sistemi informativi della Pubblica Amministrazione, le funzioni competenti, in collaborazione con i referenti interni per la gestione degli aspetti IT[10], ciascuno per gli aspetti di pertinenza, assicurano:

- un'adeguata gestione delle credenziali di accesso a detti sistemi;
- l'effettuazione di verifiche informatiche periodiche volte a garantire che l'accesso effettivo ai sistemi informatici della PA sia effettuato in funzione delle procure in essere al fine di assicurare la completezza, l'accuratezza e la veridicità della documentazione/dati/info da trasmettere o ricevere (trasmissione telematica dei dati, in modo particolare se corredata di autenticazione o firma digitale, invio dei file prodotti da elaborazioni on line, etc.).

Qualora, per specifici programmi, contratti o convenzioni, sia prevista la possibilità di ricorrere a partner commerciali esterni ad Infratel Italia, la Società assicura che la selezione del partner:

- sia autorizzata in accordo al vigente sistema di procure/deleghe interne;
- avvenga nel rispetto delle norme nazionali e comunitarie applicabili;
- avvenga previa verifica di affidabilità ed onorabilità del partner in accordo agli elementi di controllo stabiliti nel presente documento[11];
- avvenga nel rispetto dei principi di trasparenza e tracciabilità, secondo criteri basati su motivazioni di ordine tecnico/economico e/o strategico;
- preveda la formalizzazione dei principali step decisionali seguiti;
- preveda accordi contrattuali contenenti specifiche clausole di salvaguardia relative al D.Lgs. 231/01, anche

[8] I soggetti firmatari sono tenuti a sottoscrivere un'attestazione del rispetto delle regole definite nel Modello ex D.Lgs. 231/01 e nel PPCTex L. 190/12 e del Codice Etico.
[9] Devono essere formalizzate le motivazioni che hanno condotto ad eventuali aggiornamenti della Pianificazione oggetto di comunicazione formale al committente.
[10] Ovvero gli uffici competenti di Capogruppo.
[11] Anche attraverso la verifica dell'adozione di un proprio modello organizzativo e di un codice etico ai sensi del D.Lgs. 231/01

con riferimento:

- ○ all'obbligo, in capo al partner commerciale, di rilasciare periodicamente dichiarazioni di non essere a conoscenza di informazioni o situazioni che possano, direttamente o indirettamente, configurare le ipotesi di reato previste dal D.Lgs. 231/01;
- ○ alla facoltà di operare specifiche e mirate attività di audit, anche a fronte di eventuali indicatori di rischio rilevati;
- preveda l'adozione, accanto al Codice Etico, di uno specifico Codice di Comportamento che contenga le regole etico-sociali destinate a disciplinare i rapporti dei suddetti partner commerciali con Infratel Italia, cui auspicabilmente aderiscano tutti i soggetti che affiancano la Società nelle diverse opportunità di business (es. joint venture, ATI, RTI, consorzi, etc.).

Nel caso di individuazione e scelta di partner facenti capo ad enti della Pubblica Amministrazione o incaricati di pubblico servizio, la gestione dei rapporti tra i Soggetti titolati di Infratel Italia ed i rappresentanti del partner deve essere improntata nel rispetto dei codici di condotta e dei protocolli di gestione relativi ai rapporti con la Pubblica Amministrazione definiti nel presente documento.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie od atipicità riscontrate, l'Amministratore Delegato è tenuto alla comunicazione periodica, su base annuale all'OdV ed al RPCT di un'informativa riepilogativa del numero di opportunità in essere e del relativo stato di sviluppo e di una tempestiva comunicazione al Responsabile della Trasparenza di tutti i singoli nuovi contratti/accordi/convenzioni sottoscritti, al fine di adempiere agli obblighi relativi alla normativa sulla "trasparenza".

II.1.2.3. Ulteriori elementi di controllo per gestione dei rapporti con la pubblica amministrazione

Tra le attività che Infratel compie in contatto con la Pubblica Amministrazione vi è anche la partecipazione alla promozione della mission aziendale. Tale attività si manifesta come processo meramente strumentale, in quanto si tratta di eventi privi di particolari elementi di esposizione. Tuttavia, non si può escludere che lo svolgimento degli incontri possa agevolare od occultare la commissione di un illecito, né, altresì, può escludersi che i responsabili di tale attività partecipino in concorso con le funzioni coinvolte in altre ipotesi di rischio, divenendo in tal caso essi stessi direttamente autori dell'illecito.
Di seguito si riporta l'esemplificazione delle potenziali condotte illecite strumentali:

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Partecipazione alla promozione della mission aziendale	Pres./A.D./D.G./Procuratore RMC/Procuratore IO/Delegato/altri soggetti legittimati	Truffe, anche informatiche, ai danni di PA centrali e locali; peculato; peculato d'uso ed indebita destinazione quando commessi ai danni dell'UE, corruzione attiva e passiva; concussione; induzione indebita a dare o promettere denaro o altra utilità nei rapporti tra soggetti di INF e soggetti del MIMIT, del DTD, dell'ADE o altre amministrazioni centrali; istigazione alla corruzione: traffico di influenze illecite	RISCHIO STRUMENTALE: Art. 24 d.lgs. 231/2001 (artt. 640, 640-bis, 640-ter c.p.); Art. 25 d.lgs. 231/2001 (artt. 314, 314-bis, 316, 317, 318, 319, 319-quater, 321, 321, 322, 346-bis c.p.)

Al fine di prevenire gli ulteriori rischi di illecito correlati alle attività meramente strumentali, il risk owner di primo livello svolge la propria attività in coordinamento con le altre funzioni interne e della Capogruppo coinvolte, rispettando i principi generali di controllo e il codice etico, avendo come punti di attenzione i rischi strumentali sopra indicati.
Il process owner garantisce l'effettività e l'efficacia dei controlli, adeguando periodicamente le procedure. A tal fine richiede una informativa ai risk owner, sulla base della quale egli acquisisce le informazioni rilevanti per attuare le opportune azioni correttive e alimentare i flussi informativi, segnalando tempestivamente all'OdV, e al RPCT se di competenza, eventuali anomalie o non conformità riscontrate.

II.1.3. GESTIONE DEI RAPPORTI CON I SOGGETTI PRIVATI

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Scouting	Pres./A.D./D. G./ soggetti titolati	Corruzione attiva o passiva; traffico di influenze illecite; peculato e indebita destinazione ai danni dell'UE; concussione; induzione indebita a dare o promettere utilità; corruzione tra privati e istigazione alla corruzione tra privati; emissione di fatture oggettivamente o soggettivamente false	**RISCHIO DIRETTO:** **Art. 25 d.lgs. 231/2001;** **Art. 25-ter d.lgs. 231/2001 (atrt. 2635, 2635-bis c.c.);** **Art. 25-quinquiesdecies d.lgs. 231/2001 (art. 8 d.lgs. 74/2000);** **Art. 25-bis.1 d.lgs. 231/2001**
Promozione e negoziazione della cessione dei diritti di sfruttamento economico di infrastrutture	AD, soggetti titolati, BD	Concussione; corruzione passiva; induzione indebita a dare o promettere utilità; corruzione tra privati; istigazione alla corruzione tra privati; manipolazione del mercato	**RISCHIO DIRETTO:** **art. 25 d.lgs. 231/2001 (artt. 317, 318, 319,** **319-quater, 320, 322 c.p.);** **Art. 25-ter d.lgs. 231/2001 (artt. 2635, 2635-bis c.c.);** **Art. 25-sexies d.lgs. 231/2001 (art. 185 TUF)**
Comunicazione e promozione della mission aziendale verso utenti e cittadini	RPEUT, Pres, .A.D., soggetti titolati	Messa a disposizione del pubblico di un'opera dell'ingegno protetta o di parte di essa; duplicazione abusiva di programmi per elaboratore; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori; riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati; abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere scientifiche; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa; omessa segnalazione alla Autorità giudiziaria o alla P.G. di condotte penalmente rilevanti ai sensi della L. n. 633/1941, degli artt. 615-ter e 640-ter c.p.; omessa comunicazione all'AGCOM di un punto di contatto diretto; truffe, anche informatiche ai danni di PA centrali o locali; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; corruzione tra privati; aggiotaggio; manipolazione del mercato	**RISCHIO DIRETTO:** **Art. 25-novies d.lgs 231/2001 (artt. 171, 171-bis, 171-ter, 174-sexies l. 633/1941)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs. 231/2001** **(artt. 640, 640-bis, 640-ter c.p.); Art. 25 d.lgs. 231/2001** **(artt. 317, 318, 319, 319-quater, 320, 322 c.p.);** **art. 25-ter d.lgs. 231/2001 (artt. 2635, 2635-bis, 2637, c.c.);** **art. 25-sexies d.lgs. 231/2001 (art. 185 TUF)**

II.1.4. ELEMENTI DI CONTROLLO GESTIONE DEI RAPPORTI CON I SOGGETTI PRIVATI

II.1.4.1. Promozione e negoziazione della cessione dei diritti di sfruttamento di infrastrutture. Scouting tecnologico

Il sistema di procure e deleghe definisce i soggetti titolati a intrattenere rapporti di tipo economico e non, con soggetti privati, per conto di Infratel Italia.

Gli eventuali incontri devono essere condotti nel rispetto del Codice Etico e, in particolare, in ottemperanza alle seguenti prescrizioni:

- non è consentito a coloro che operano per conto di Infratel Italia, direttamente o indirettamente, né per il tramite di interposta persona, ricevere denaro, doni, favori, compensi o altra utilità, sotto qualsiasi forma, che possano influenzare il proprio giudizio nell'ambito di qualsiasi tipologia di rapporto con soggetti terzi rilevanti quali, a titolo indicativo, committenti, concessionari, beneficiari, affidatari, cessionari;
- è fatto obbligo di instaurare e gestire qualsiasi rapporto sulla base di criteri di massima correttezza, imparzialità, trasparenza e buona fede, nel rispetto del codice delle telecomunicazioni, dei principi di concorrenza e rotazione;
- non è consentito abusare della propria qualità per ottenere vantaggi patrimoniali o non patrimoniali, nelle attività svolte per conto di Infratel Italia;
- non è consentito utilizzare o presentare dichiarazioni e documenti attestanti fatti e notizie non vere, ovvero omettere informazioni per conseguire l'aggiudicazione di un contratto/convenzione/finanziamento/erogazione o l'approvazione di un rapporto rendicontativo, nonché qualsiasi attività/operazione/atto a vantaggio o nell'interesse di Infratel Italia.

Gli incontri con i rappresentanti di soggetti beneficiari privati, concessionari, affidatari, cessionari, appaltatori e sub-appaltatori, partner commerciali, quali meeting di natura decisionale o programmatica, strumentali o finalizzati alla formalizzazione di atti/contratti/convenzioni, ovvero alla ricerca di nuove soluzioni tecnologiche, oppure legati a Stati Avanzamento Lavori prodromici al processo di rendicontazione verso il committente o comunque legati all'accettazione della prestazione o servizio erogati dalla Società, devono essere presenziati preferibilmente da due rappresentanti di Infratel Italia. Di detti incontri deve comunque essere redatto apposito verbale. Tali informazioni devono essere comunicate al proprio responsabile e al RPCT[12], quindi archiviate e conservate.

Qualora, per specifici programmi, contratti o convenzioni, sia prevista la possibilità di ricorrere a partner commerciali esterni ad Infratel Italia, la Società assicura che la selezione del partner avvenga con le medesime modalità descritte nel paragrafo "Contratti/accordi/convenzioni e affidamenti con soggetti pubblici committenti".

Fermo restando l'obbligo in capo a tutti gli attori coinvolti di comunicare eventuali anomalie o atipicità riscontrate, chiunque riceva offerte o promesse esplicite o implicite di benefici o utilità di qualsiasi natura da parte di soggetti privati, anche attraverso interposta persona, atte a turbare l'esercizio imparziale del servizio pubblico o della funzione che il destinatario del Modello svolge (es.: funzione di RUP), o comunque per il compimento di atti in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà verso la Società, è tenuto ad informare tempestivamente l'OdV ed il RPCT, quindi a sospendere immediatamente ogni rapporto con essi.

II.1.4.2. Comunicazione e promozione della mission aziendale verso utenti e cittadini

Infratel Italia assicura nell'ambito della comunicazione esterna il rispetto della normativa applicabile in materia di diritto d'autore.

Qualora si renda necessario diffondere una comunicazione all'esterno, la Funzione Comunicazione presso la Capogruppo elabora le comunicazioni oggetto di diffusione, da sottoporre a verifica e approvazione da parte dei Soggetti titolati della Società prima dell'emissione definitiva.

Ai suddetti Soggetti titolati è fatto assoluto divieto di diffondere informazioni, voci e notizie non corrette, non aggiornate o in generale false o fuorvianti direttamente o indirettamente concernenti la Società, anche quando possano avere un impatto significativo sul mercato del risparmio.

[12] Secondo le tempistiche dallo stesso definite. Le motivazioni di eventuali deroghe alla predisposizione della sintesi degli incontri sono oggetto di comunicazione tempestiva al RPCT.

La Funzione Comunicazione presso la Capogruppo sovraintende e garantisce:

- la diffusione di codici di condotta da utilizzarsi per la preparazione dei contenuti oggetto di pubblicazione, atti a vietare la duplicazione oltre i limiti di legge e la distribuzione di testi ed immagini protetti dal diritto di autore;
- qualora vengano pubblicati contenuti informativi o immagini di terzi, l'ottenimento delle opportune autorizzazioni da parte dell'autore o dei soggetti detentori dei relativi diritti;
- anche in collaborazione con la funzione Affari Legali presso la Capogruppo, la presenza, nei contratti stipulati con soggetti terzi fornitori di testi o immagini, di specifiche clausole inerenti al diritto d'autore e il trattamento dei dati personali.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate, la funzione Comunicazione presso la Capogruppo è tenuta ad inviare all'OdV, per mezzo dell'Amministratore Delegato di Infratel Italia, un'informativa periodica, su base annuale, riepilogativa delle comunicazioni effettuate durante l'anno a mezzo web o stampa, con l'indicazione per ciascuna di esse della sintesi del contenuto e dei destinatari.

II.1.4.3. Ulteriori elementi di controllo per gestione dei rapporti con i soggetti privati

Tra i soggetti esterni con cui la Società ha dei rapporti rientra sicuramente la Società Capogruppo, Invitalia. Nei confronti di essa, Infratel Italia è soggetta ad attività di audit e di reportistica ai fini del monitoraggio da parte della Controllante. L'invio di report verso la Capogruppo si manifesta come processo meramente strumentale, in quanto funzionale al monitoraggio da parte di Invitalia per lo svolgimento delle attività di audit.
Tuttavia, non si può escludere che una grave carenza nello svolgimento dell'attività possa agevolare od occultare la commissione di un illecito, né, altresì, può escludersi che i responsabili dell'invio dei report partecipino in concorso con le funzioni coinvolte in altre ipotesi di rischio, divenendo in tal caso essi stessi direttamente autori dell'illecito.
Di seguito si riporta l'esemplificazione delle potenziali condotte illecite strumentali:

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Report nei confronti della Capogruppo	Responsabile della/e funzione/i coinvolta/e, controllo di gestione, Internal Auditing	false comunicazioni sociali, ostacolo al controllo dei soci o degli organi sociali, restituzione indebita di conferimenti ai soci, ripartizione illegale degli utili, operazioni illecite su azioni o quote sociali, operazioni dolose in danno dei creditori, formazione fittizia del capitale, corruzione tra privati, determinazione fraudolenta della maggioranza assembleare, aggiotaggio, ostacolo alle attività di vigilanza di pubbliche autorità; abuso di informazioni privilegiate, manipolazione del mercato; omicidio colposo aggravato dalla violazione delle norme sulla prevenzione degli infortuni sul lavoro, lesioni gravi o gravissime aggravate dalla violazione delle norme sulla prevenzione degli infortuni sul lavoro; ricettazione, riciclaggio, reimpiego in attività produttive, autoriciclaggio di beni di provenienza di provenienza illecita; inquinamento ambientale, disastro ambientale, inquinamento e disastro ambientale colposi, uccisione di spese animali o vegetali protette, distruzione di un habitat all'interno di un sito protetto;impiego di cittadini di paesi terzi irregolari, favoreggiamento della permanenza illegale dello straniero; reati in materia doganale; furto di beni culturali, appropriazione indebita di beni culturali, ricettazione di beni culturali, falsificazione in scrittura privata relativa a beni culturali, violazione non autorizzata di beni culturali/omessa denuncia di cessione, importazione ed esportazione illecita	Rischio strumentale: Art. 25-ter d.lgs. 231/2001; art. 25-sexies d.lgs. 231/2001; art. 25-septies d.lgs. 231/2001; art. 25-octies d.lgs. 231/2001; a art. 25-undecies d.lgs. 231/2001; art. 25-duodecies d.lgs. 231/2001; art. 25-quinquiesdecies d.lgs. 231/2001; art. 25-sexiesdecies d.lgs. 231/2001; art. 25-septiesdecies d.lgs. 231/2001; art. 25-duodevicies d.lgs. 231/2001.

		di beni culturali, distruzione di beni culturali, contraffazione di beni culturali; riciclaggio di beni culturali, devastazione o sacchieggio di beni culturali;	

Al fine di prevenire gli ulteriori rischi di illecito correlati alle attività meramente strumentali, il risk owner di primo livello svolge la propria attività in coordinamento con le altre funzioni interne e della Capogruppo coinvolte, rispettando i principi generali di controllo e il codice etico, avendo come punti di attenzione i rischi strumentali sopra indicati.
Il process owner garantisce l'effettività e l'efficacia dei controlli, adeguando periodicamente le procedure. A tal fine richiede una informativa ai risk owner, sulla base della quale egli acquisisce le informazioni rilevanti per attuare le opportune azioni correttive e alimentare i flussi informativi, segnalando tempestivamente all'OdV, e al RPCT se di competenza, eventuali anomalie o non conformità riscontrate.

II.1.5. GESTIONE DEI FINANZIAMENTI, DEI FONDI E DELLE CONCESSIONI

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Richiesta di finanziamenti/fondi	A.D.	Malversazioni di fondi pubblici; indebita percezione di erogazioni pubbliche; truffe, anche informatiche; ai danni di PA centrali o locali; concussione; corruzione attiva o passiva; istigazione alla corruzione; induzione indebita a dare o promettere utilità, corruzione attiva e passiva, corruzione in atti giudiziari, istigazione alla corruzione - di membri degli organi UE o di funzionari UE; traffico di influenze illecite; falsità in documento pubblico informatico; peculato, peculato d'uso ed indebita destinazione quando commessi ai danni dell'UE; ricettazione; riciclaggio; reimpiego in attività produttive; autoriciclaggio di beni di provenienza illecita	**RISCHIO DIRETTO:** **Art. 24 d.lgs. 231/2001 (artt. 316-bis, 316-ter, 640, 640-bis, 640-ter c.p.);** **Art. 25 d.lgs. 231/2001 (artt. 317, 318, 319, 319-quater, 320, 322, 322-bis, 346-bis c.p.)** **RISCHIO STRUMENTALE:** **Art. 24-bis d.lgs. 231/2001 (art. 491-bis c.p.);** **Art. 25 d.lgs. 231/2001 (artt. 314, 314-bis, 316 c.p.);** **Art. 25-octies D. lgs. 231/2001**
Impiego dei finanziamenti/fondi	C.D.A./A.D./resp. Pianificazione Gare e ingegneria/Resp. funzioni coinvolte	Malversazioni di fondi pubblici; indebita percezioni di erogazioni pubbliche; truffe, anche informatiche, ai danni di PA centrali o locali; peculato, destinazione indebita e peculato d'uso quando commessi ai danni dell'UE; concussione; corruzione attiva o passiva; corruzione in atti giudiziari; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; false comunicazioni sociali; ostacolo al controllo dei soci o degli organi sociali; restituzione indebita di conferimenti ai soci; ripartizione illegale degli utili; operazioni illecite su azioni o quote sociali; operazioni dolose in danno dei creditori; formazione fittizia del capitale; corruzione tra privati; determinazione fraudolenta della maggioranza assembleare; aggiotaggio; ostacolo alle attività di vigilanza di pubbliche autorità; ricettazione; riciclaggio; reimpiego in attività produttive; autoriciclaggio di beni di provenienza illecita	**RISCHIO DIRETTO:** **Art. 24 d.lgs. 231/2001 (artt. 316-bis, 316-ter,** **640, 640-bis, 640-ter c.p.);** **Art. 25 d.lgs. 231/2001 (artt. 314, 314-bis, 316 c.p.)** **RISCHIO STRUMENTALE:** **Art. 25 d.lgs. 231/2001 (ad eccezione degli** **artt. 314, 314-bis, 316, 322-bis c.p.);** **Art. 25-ter d.lgs. 231/2001;** **Art. 25-octies d. lgs. 231/2001**

Rendicontazione dei finanziamenti/fondi	A.D.; D.G./resp. Rendicontazione	Malversazione di fondi pubblici; indebita percezione di erogazioni pubbliche; corruzione di un appartenente all'AG; truffe, anche informatiche, ai danni di PA centrali o locali; peculato, peculato d'uso e destinazione indebita ai danni dell'UE; falsità in documento pubblico informatico; ostacolo al controllo dei soci o degli organi sociali; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza corruzione tra privati; ricettazione; riciclaggio; reimpiego in attività produttive; autoriciclaggio di beni di provenienza di provenienza illecita; uso nelle dichiarazioni relative alle imposte sui redditi o all'IVA di fatture oggettivamente o soggettivamente false; dichiarazione infedele o omessa per importi superiori alle soglie di punibilità; emissione di fatture oggettivamente o soggettivamente false; distruzione o occultamento di documenti contabili; compensazione indebita ai danni dell'UE; sottrazione fraudolenta alle procedure erariale di riscossione coattiva	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 640, 640-bis, 640-ter c.p.);** **Art. 25 d.lgs. 231/2001 (artt. 314, 314-bis, 316 c.p.);** **24-bis d.lgs. 231/2001 (art. 491-bis c.p.);** **Art. 25-ter d.lgs. 231/2001 (artt. 2625, 2638 c.c.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs. 231/2001 (artt. 316-bis, 316-ter c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635 c.c.)** **Art. 25-octies d.lgs 231/2001** **Art. 25-quinquiesdecies d.lgs 231/2001**
Erogazione dei finanziamenti a incentivo e concessioni	A.D.; responsabile Ufficio Pianificazione Gare e ingegneria; resp. Infrastrutture e Operations, resp. Reti Mobili e Connettivita', R.U.P.	Malversazione di fondi pubblici; percezione indebita di erogazioni pubbliche; turbata libertà degli incanti; turbata libertà del processo di scelta del contraente; frode nelle pubbliche forniture; truffe, anche informatiche, ai danni di PA centrali o locali; peculato; destinazione indebita e peculato d'uso quando commessi ai danni dell'UE; concussione; corruzione attiva o passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione tra privati; riciclaggio; reimpiego di beni di provenienza illecita; falsità in documento pubblico informatico; accesso abusivo a sistema informatico o telematico; danneggiamento di dati o programmi informatici anche di interesse pubblico	**RISCHIO DIRETTO:** **Art. 24 d.lgs. 231/2001** **Art. 25 d. lgs. 231/2001 (ad eccezione degli artt. 319-ter, 322-bis c.p.);** **Art. 25-ter (art. 2635 c.c.);** **Art. 25 octies (artt. 648-bis, 648-ter c.p.)** **RISCHIO STRUMENTALE:** **Art. 24-bis d.lgs. 231/2001 (art. 491-bis, 615-ter, 635-bis, 635-ter c.p.)**

II.1.6. ELEMENTI DI CONTROLLO GESTIONE DEI FINANZIAMENTI

II.1.6.1. Richiesta ed utilizzo di finanziamenti/agevolazioni pubbliche

Infratel Italia assicura correttezza, trasparenza e veridicità nella predisposizione e presentazione di dichiarazioni/documenti attestanti fatti e notizie finalizzate all'ottenimento di un finanziamento/erogazione pubblica. In occasione della realizzazione di un progetto per cui si configuri l'opportunità di ottenere un finanziamento pubblico, il Responsabile della funzione aziendale interessata sottopone il progetto al Presidente/Amministratore Delegato per ottenere l'autorizzazione a procedere in qualità di "Responsabile dell'operazione", anche formalmente titolato a gestire i rapporti con l'ente pubblico erogatore.

Il Responsabile dell'operazione cura la fase di raccolta della documentazione necessaria e la successiva trasmissione all'ente erogatore, previa autorizzazione e sottoscrizione da parte dell'Amministratore Delegato e/o dei Soggetti titolati della Società[13]; è previsto che il Responsabile dell'operazione possa richiedere dati e informazioni alle Funzioni interne competenti al fine di predisporre la documentazione necessaria. Dette informazioni, fornite in modo tracciato dalle funzioni competenti al Responsabile dell'operazione, devono essere verificate dai rispettivi Responsabili che ne assicurano la correttezza e veridicità.

La fase di gestione del finanziamento erogato prevede che il Responsabile dell'operazione, ovvero il

[13] I soggetti firmatari ovvero il Responsabile dell'operazione se diverso, sono tenuti a sottoscrivere un'attestazione del rispetto delle regole definite nel Modello 231, Parte Generale e Parte Speciale ex D.Lgs. 231/01 e nel PPC ex L. 190/12 e del Codice Etico

Responsabile di Commessa/Progetto qualora il progetto origini una Commessa/Progetto, anche avvalendosi della collaborazione degli Uffici competenti, effettui un monitoraggio, in termini di tempo e risorse dedicate, dell'attività finanziata in relazione al progetto approvato. I risultati di detto monitoraggio sono comunicati all'Amministratore Delegato. La fase di Rendicontazione è svolta secondo le modalità stabilite per il processo di Rendicontazione.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate, l'Amministratore Delegato è tenuto alla comunicazione periodica, su base annuale, all'Organismo di Vigilanza e al RPCT di un'informativa riepilogativa dello stato dei finanziamenti in corso.

II.1.6.2. Erogazione dei finanziamenti

Infratel Italia assicura correttezza, trasparenza e tracciabilità nell'esecuzione delle attività preordinate alla gestione e al controllo dei finanziamenti erogati nel rispetto degli accordi formali stipulati con il committente. Con riferimento alle Commesse di tipo incentivo deve essere garantita segregazione funzionale tra chi svolge le attività di attuazione e gestione, ivi incluso il monitoraggio, e chi svolge l'attività di controllo nella fase di rendicontazione.

Per tutti i progetti che prevedono un contratto/convenzione stipulato tra Infratel Italia ed il beneficiario/assegnatario del finanziamento, si rinvia ad un Piano di dettaglio delle attività, predisposto dalla società beneficiaria coerentemente ai requisiti del bando ed a quanto delineato in fase di proposta di ammissione al finanziamento. Tale piano è oggetto di revisione periodica in corso di erogazione del finanziamento e viene sottoposto ad autorizzazione da parte dell'Ufficio competente per l'erogazione del finanziamento e/o dell'Amministratore Delegato ad ogni aggiornamento.

L'erogazione dei finanziamenti avviene ad opera delle funzioni preposte di Infratel Italia, nel rispetto degli elementi di controllo stabiliti per il processo di Gestione della Tesoreria nell'ambito dell'area Amministrazione e Bilancio, previa acquisizione:

- degli esiti della verifica, ad opera dell'Ufficio Rendicontazione, di rispondenza, completezza, correttezza ed effettività del prospetto rendicontativo prodotto dal beneficiario, in accordo alle linee guida di rendicontazione, elaborate dall'Ufficio Rendicontazione[14], approvate dall'Amministratore Delegato e oggetto di comunicazione al beneficiario;
- del mandato di pagamento emesso dall'Ufficio competente per l'erogazione del finanziamento a fronte della ricezione e verifica degli atti/documenti, predisposti dal Responsabile dell'operazione/Commessa/Progetto con il supporto di suddetti soggetti/funzioni responsabili della verifica del corretto operato del beneficiario;
- della documentazione attestante eventuali condizioni sospensive, tra cui quelle legate alle inadempienze del beneficiario o a vizi in termini di affidabilità/onorabilità dello stesso, rilevata, anche in corso di gestione del rapporto, dagli Uffici competenti della Società;
- nel caso di SAL intermedi e finali, dell'autorizzazione al pagamento da parte degli enti preposti a fronte di un report[15] di monitoraggio e rendicontazione, elaborato dall'Ufficio Rendicontazione e dal Responsabile di commessa/progetto, quindi approvato e comunicato formalmente agli enti dai Soggetti titolati della Società, contenente i dati di avanzamento, il riepilogo dei costi sostenuti, la tipologia dei controlli effettuati e tutto il materiale a supporto consegnato ad Infratel Italia dal beneficiario.

L'Ufficio competente per l'erogazione del finanziamento assicura, anche per il tramite delle funzioni/soggetti interni da questa identificati, in collaborazione con il Responsabile di Commessa/RUP, la pianificazione e

[14] In accordo ai contratti/accordi applicabili ed alle modalità previste dal bando

[15] Ovvero i soggetti diversi dai membri componenti la suddetta commissione di valutazione

l'attuazione di verifiche sistematiche, atte ad attestare il corretto operato dell'assegnatario nel rispetto del Piano delle attività, nonché a certificare la conformità delle spese sostenute con quanto dichiarato dal beneficiario stesso.

I risultati di tali verifiche sono comunicati alle funzioni interne interessate per le attività di pertinenza anche finalizzate all'erogazione dei finanziamenti in accordo al raggiungimento degli Stati Avanzamento Lavori predefiniti, nonché tempestivamente all'Amministratore Delegato ed alle funzioni interne interessate, in caso di anomalie rilevate, per le eventuali opportune azioni correttive.

Tutti gli atti formali relativi alle decisioni stabilite da Infratel Italia nelle diverse fasi del processo di gestione/erogazione del finanziamento, tra cui le delibere di ammissione/revoca/risoluzione, le note di attuazione/decadenza, il contratto con il beneficiario, ed il mandato di pagamento sono sottoposti ad autorizzazione dell'Amministratore Delegato, quindi comunicati dai Soggetti titolati della Società al proponente/beneficiario.

Le funzioni interne preposte elaborano la documentazione di supporto alle attività di monitoraggio e controllo (i.e. piste di controllo), in conformità a quanto stabilito nella convenzione di riferimento, oggetto di invio formale da parte dei Soggetti titolati della Società agli enti preposti per verifica ed approvazione.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate, il Responsabile dell'operazione di finanziamento è tenuto alla comunicazione periodica, su base annuale, all'Organismo di Vigilanza ed al RPCT di un'informativa riepilogativa di eventuali anomalie rilevate durante il monitoraggio dell'operato dei beneficiari e delle relative azioni stabilite.

In ogni caso, i responsabili degli Uffici interessati, con cadenza almeno annuale, comunicano all'OdV e al RPCT le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

II.1.6.3. Ulteriori elementi di controllo per gestione dei finanziamenti

L'attività di ricerca dei finanziamenti, analoga per alcuni aspetti a quella di scouting, è meramente strumentale, in quanto prodromica alle situazioni fattuali che potrebbero dar luogo a potenziali illeciti.
Tuttavia, non si può escludere che l'inosservanza delle regole di condotta nello svolgimento della stessa possa agevolare od occultare la commissione di un illecito, né, altresì, può escludersi che i responsabili di tale funzione partecipino in concorso con le funzioni coinvolte in altre ipotesi di rischio, divenendo in tal caso essi stessi direttamente autori dell'illecito.
Di seguito si riporta l'esemplificazione delle potenziali condotte illecite strumentali:

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Ricerca di finanziamenti/fondi	A.D./resp. Pianificazione /resp. PGI/resp. BD	Malversazioni di fondi pubblici; indebita percezioni di erogazioni pubbliche; truffe, anche informatiche, ai danni di PA centrali o locali; concussione; corruzione attiva o passiva; istigazione alla corruzione; induzione indebita a dare o promettere utilità, corruzione attiva e passiva, corruzione in atti giudiziari, istigazione alla corruzione - di membri degli organi UE o di funzionari UE; traffico di influenze illecite	RISCHIO STRUMENTALE: Art. 24 d.lgs. 231/2001 (artt. 316-bis, 316-ter, 640, 640-bis, 640-ter c.p.); Art. 25 d.lgs. 231/2001 (artt. 317, 318, 319, 319-quater, 320, 322, 322-bis, 346-bis c.p.)

Al fine di prevenire gli ulteriori rischi di illecito correlati alle attività meramente strumentali, il risk owner di primo livello svolge le proprie attività in coordinamento con le altre funzioni interne e della Capogruppo coinvolte, rispettando i principi generali di controllo e il codice etico, avendo come punti di attenzione i rischi strumentali sopra indicati.

Il process owner garantisce l'effettività e l'efficacia dei controlli, adeguando periodicamente le procedure. A tal fine richiede una informativa ai risk owner, sulla base della quale egli acquisisce le informazioni rilevanti per attuare le opportune azioni correttive e alimentare i flussi informativi, segnalando tempestivamente all'OdV, e al RPCT se di competenza, eventuali anomalie o non conformità riscontrate.

II.1.7. GESTIONE DEGLI ADEMPIMENTI NEI CONFRONTI DELLE AUTORITÀ PUBBLICHE E DEGLI ORGANI DI CONTROLLO

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Gestione degli adempimenti fiscali	Pres./A.D./CDA/A.D./referente service Capogruppo	Uso nelle dichiarazioni relative alle imposte sui redditi o all'IVA di fatture oggettivamente o soggettivamente false; dichiarazione infedele o omessa per importi superiori alle soglie di punibilità; emissione di fatture oggettivamente o soggettivamente false; distruzione o occultamento di documenti contabili; compensazione indebita ai danni dell'UE; sottrazione fraudolenta alle procedure erariale di riscossione coattiva; ricettazione; riciclaggio; reimpiego in attività produttive; autoriciclaggio di beni di provenienza illecita	**RISCHIO DIRETTO: Art. 25-quinquiesdecies d.lgs. 231/2001** **RISCHIO STRUMENTALE: Art. 25-octies d.lgs. 231/2001**
Comunicazioni obbligatorie alle Autorità di Vigilanza o altre PPAA	Pres./CDA/A.D./D.G./delegato	Falsità in documento pubblico informatico; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; malversazione di fondi pubblici; percezione indebita di erogazioni pubbliche; turbata libertà degli incanti; turbata libertà del processo di scelta del contraente; frode nelle pubbliche forniture; truffe, anche informatiche, ai danni di PA centrali o locali; peculato, destinazione indebita e peculato d'uso quando commessi ai danni dell'UE; ricettazione; riciclaggio; reimpiego in attività produttive; autoriciclaggio di beni di provenienza di provenienza illecita; inquinamento ambientale; disastro ambientale; inquinamento e disastro ambientale colposi; uccisione di specie animali o vegetali protette; distruzione di un habitat all'interno di un sito protetto; impiego di cittadini di paesi terzi irregolari; favoreggiamento della permanenza illegale dello straniero; uso nelle dichiarazioni relative alle imposte sui redditi o all'IVA di fatture oggettivamente o soggettivamente false; dichiarazione infedele o omessa per importi superiori alle soglie di punibilità, emissione di fatture oggettivamente o soggettivamente false; distruzione o occultamento di documenti contabili; compensazione indebita ai danni dell'UE; sottrazione fraudolenta alle procedure erariale di riscossione coattiva; reati in materia doganale; furto di beni culturali; appropriazione indebita di beni culturali; ricettazione di beni culturali; falsificazione in scrittura privata relativa a beni culturali; vendita non autorizzata di beni culturali/omessa denuncia di cessione; importazione ed esportazione illecita di beni culturali; distruzione di beni culturali; contraffazione di beni culturali; riciclaggio di beni culturali; devastazione o saccheggio di beni culturali	**RISCHIO DIRETTO: Art. 24-bis d.lgs. 231/2001 (art. 491-bis c.p.) Art. 25-ter d.lgs. 231/2001 (art. 2638 c.c.)** **RISCHIO STRUMENTALE: Art. 24 d.lgs. 231/2001; Art. 25 d.lgs. 231/2001 (artt. 314, 314-bis, 316 c.p.) Art. 25-octies d.lgs. 231/2001; Art. 25-undecies d.lgs. 231/2001 (artt. 452-bis, 452-quater, 452-quinquies, 727-bis, 733-bis c.p.); Art. 25-duodecies d.lgs. 231/2001; Art. 25-quinquiesdecies d.lgs. 231/2001; Art. 25-sexiesdecies d.lgs. 231/2001; Art. 25-septiesdecies d.lgs. 231/2001 (ad eccezione art. 518-quaterdecies); Art. 25-duodevicies d.lgs. 231/2001**
Attività poste in essere in occasione di visite ispettive o accertamenti da parte di pubbliche autorità	Pres./A.D./D.G./CDA/CS/Responsabile della/e funzione/i coinvolta/e	Concussione; corruzione attiva o passiva; istigazione alla corruzione;induzione indebita a dare o promettere utilità, corruzione attiva e passiva, corruzione in atti giudiziari, istigazione alla corruzione - di membri degli organi UE o di funzionari UE; traffico di influenze illecite malversazione di fondi pubblici; percezione indebita di erogazioni pubbliche; turbata libertà degli incanti; turbata libertà del processo di scelta del contraente; frode nelle pubbliche forniture; truffe, anche informatiche, ai danni di PA centrali o locali; peculato, destinazione indebita e peculato d'uso quando commessi ai danni dell'UE; corruzione attiva o passiva; corruzione in atti giudiziari; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; ricettazione; riciclaggio; reimpiego in attività produttive; autoriciclaggio di beni di provenienza di provenienza illecita; inquinamento ambientale; disastro ambientale; inquinamento e disastro ambientale colposi; uccisione di specie animali o vegetali protette; distruzione di un habitat all'interno di un sito protetto; impiego di cittadini di paesi terzi irregolari; favoreggiamento della permanenza illegale dello straniero; uso nelle	**RISCHIO DIRETTO: Art. 25 d.lgs. 231/2001 (artt. 317, 318, 319, 319-quater, 320, 322, 322-bis, 346-bis c.p.)** **RISCHIO STRUMENTALE: Art. 24 d.lgs. 231/2001; Art. 25 d.lgs. 231/2001 (art. 314, 314-bis, 316 c.p.) Art. 25-octies d.lgs. 231/2001; Art. 25-undecies d.lgs. 231/2001 (artt. 452-bis, 452-quater, 452-quinquies, 727-bis, 733-bis c.p.); Art. 25-duodecies d.lgs. 231/2001; Art. 25-quinquiesdecies d.lgs. 231/2001; Art. 25-sexiesdecies d.lgs. 231/2001; Art. 25-septiesdecies d.lgs. 231/2001 (ad eccezione art. 518-**

		dichiarazioni relative alle imposte sui redditi o all'IVA di fatture oggettivamente o soggettivamente false; dichiarazione infedele o omessa per importi superiori alle soglie di punibilità; emissione di fatture oggettivamente o soggettivamente false; distruzione o occultamento di documenti contabili; compensazione indebita ai danni dell'UE; sottrazione fraudolenta alle procedure erariali di riscossione coattiva; reati in materia doganale; furto di beni culturali; appropriazione indebita di beni culturali; ricettazione di beni culturali; falsificazione in scrittura privata relativa a beni culturali; violazione non autorizzata di beni culturali/omessa denuncia di cessione; importazione ed esportazione illecita di beni culturali; distruzione di beni culturali; contraffazione di beni culturali; riciclaggio di beni culturali; devastazione o saccheggio di beni culturali	**quaterdecies);** **Art. 25-duodevicies d.lgs. 231/2001**

II.1.8. ELEMENTI DI CONTROLLO PER LA GESTIONE DEGLI ADEMPIMENTI NEI CONFRONTI DELLE AUTORITÀ PUBBLICHE E DEGLI ORGANI DI CONTROLLO

Infratel Italia assicura che gli adempimenti nei confronti delle autorità pubbliche e degli organi di controllo e la predisposizione della relativa documentazione siano effettuati con la **massima diligenza e professionalità** in modo da **fornire informazioni chiare, accurate, complete e veritiere, nel rispetto delle normative vigenti, nazionali o comunitarie**.

L'istanza per la richiesta di autorizzazioni amministrative, licenze, concessioni è firmata dal Direttore Generale o da altro personale interno, munito di procura, il quale assicura altresì la correttezza e l'affidabilità del processo di produzione della documentazione.

I Responsabili delle Funzioni aziendali coinvolte nella produzione della documentazione sono tenuti alla verifica della veridicità, correttezza, completezza e aggiornamento della documentazione predisposta e comunicata agli uffici competenti.

Le Funzioni interessate assicurano, qualora previsto, il **rispetto delle scadenze** degli adempimenti di pertinenza, anche attraverso l'utilizzo di opportuni calendari/scadenzari. **Tutta la documentazione** prodotta nell'ambito della propria attività, ivi inclusa una copia di quella trasmessa agli uffici competenti, è archiviata tramite il Protocollo informatico. Si deve inoltre prendere nota di **eventuali ulteriori contatti informali con esponenti della Pubblica Amministrazione** coinvolti nel procedimento di concessione e/o autorizzazione.

Infratel Italia **assicura piena ed immediata collaborazione con le autorità pubbliche o gli organi di vigilanza e controllo** (es. Guardia di Finanza, INAIL, Ispettorato del Lavoro, Agenzia delle Entrate) nonché il rispetto dei principi di **trasparenza e correttezza nei rapporti** con gli stessi, nel corso dei processi di verifica implementati per la realizzazione degli interventi, quali l'accoglimento della richiesta di informazioni o della visita ispettiva, l'accertamento e la **verbalizzazione**; Infratel Italia garantisce altresì la tracciabilità delle comunicazioni, delle decisioni e degli esiti dell'attività di verifica esterna.

L'Amministratore Delegato identifica i Soggetti titolati, anche per il tramite di opportune deleghe interne, a scambiare comunicazioni formali con gli organi di controllo, in funzione della tipologia e delle finalità dell'indagine/verifica.

Nel caso di accesso o richieste da parte **di enti quali Antitrust, AGCOM, ANAC, Corte dei conti, Autorità Giudiziaria, Guardia di Finanza e Pubblica Sicurezza**, il Soggetto titolato, ove necessario, chiede il **supporto dell'Ufficio Affari Legali presso la Capogruppo**. Nella fase di gestione della verifica ispettiva, il Soggetto titolato mette **a disposizione** degli ispettori **almeno due addetti della Società,** che affiancano e supportano tutte le attività di verifica esterna. **Qualsiasi richiesta** di documentazione da parte dei funzionari preposti deve **transitare attraverso il Soggetto titolato**; qualora quest'ultimo non sia nelle condizioni di produrre la

documentazione richiesta, questi dovrà attivarsi per **chiedere in modo formale e tracciato, alle funzioni competenti di Infratel Italia, la documentazione necessaria**. I dati e le informazioni richieste vengono fornite in modo tracciato dalle Funzioni competenti previa **verifica da parte dei rispettivi Responsabili,** i quali ne assicurano la correttezza, veridicità e aggiornamento.

Il **Soggetto titolato, incaricato della gestione della verifica ispettiva, è tenuto a sottoscrivere il verbale di ispezione rilasciato dall'Ente di Controllo** e a tenere traccia dell'esito della verifica nonché copia della documentazione richiesta e consegnata.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate, ciascun Responsabile di Funzione è tenuto ad informare l'Organismo di Vigilanza ed il RPCT:

- tempestivamente circa l'avvio, da parte dell'Autorità giudiziaria, di un'indagine nei confronti del personale, dei consulenti o altri partner di Infratel Italia o in cui la stessa sia stata coinvolta a seguito di una verifica ispettiva;
- deve inoltre comunicare, con cadenza annuale, attraverso un'informativa riepilogativa, l'esito e lo stato delle verifiche ispettive svolte.

L'Amministratore Delegato riepiloga le informazioni di cui al punto precedente in un report informativo da presentare con cadenza annuale all'Organismo di Vigilanza.

In ogni caso, i responsabili degli Uffici interessati, con cadenza almeno annuale, comunicano all'OdV e al RPCT le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

CAPITOLO III MISURE SPECIFICHE PER I PROCESSI GESTIONALI E DI SUPPORTO DI SECONDO LIVELLO

III.1 CONTROLLO DI GESTIONE

III.1.1. ATTIVITÀ A RISCHIO E POTENZIALI REATI

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Gestione ed esecuzione del processo di elaborazione del budget aziendale	A.D., CDA, CDS, responsabile di funzione, responsabile funzione Amministrazione e bilancio Capogruppo	Corruzione attiva o passiva; corruzione in atti giudiziari; induzione indebita a dare o promettere utilità; istigazione alla corruzione; corruzione tra privati; istigazione alla corruzione tra privati; ostacolo alle attività di vigilanza di pubbliche autorità; peculato, peculato mediante profitto dell'errore altrui e indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; traffico di influenze illecite; omicidio o lesioni gravi e gravissime aggravati dalla violazione delle norme sulla prevenzione degli infortuni sul lavoro e delle malattie professionali	**RISCHIO DIRETTO:** **Art. 25 D.Lgs. 231/2001 (artt. 318, 319, 319 ter, 319-quater, 320, 321, 322 c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis, 2638 c.c.)** **RISCHIO STRUMENTALE:** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 346-bis c.p.)** **Art. 25-septies d.lgs 231/2001**
Controlling e reporting direzionale, tramite elaborazione di previsioni, consuntivi, analisi di cash-flow, ecc.	Responsabile di funzione	Corruzione tra privati; istigazione alla corruzione tra privati; ostacolo alle attività di vigilanza di pubbliche autorità;	**RISCHIO DIRETTO:** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis, 2638 c.c.)**
Controllo dell'andamento economico della Società effettuando le analisi degli scostamenti	A.D., CDS, responsabile di funzione	Corruzione tra privati; istigazione alla corruzione tra privati; ostacolo alle attività di vigilanza di pubbliche autorità; peculato, peculato mediante profitto dell'errore altrui e indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione attiva o passiva; corruzione in atti giudiziari; induzione indebita a dare o promettere utilità; istigazione alla corruzione; induzione indebita a dare o promettere utilità, corruzione attiva e passiva, corruzione in atti giudiziari, istigazione alla corruzione - di membri degli organi UE o di funzionari UE; traffico di influenze illecite; omicidio o lesioni gravi e gravissime aggravati dalla violazione delle norme sulla prevenzione degli infortuni sul lavoro e delle malattie professionali	**RISCHIO DIRETTO:** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis, 2638 c.c.)** **RISCHIO STRUMENTALE:** **Art. 25 d.lgs 231/2001;** **Art. 25-septies d.lgs 231/2001**
Monitoraggio del livello di conseguimento degli obiettivi aziendali (KPI, indicatori di processo, ecc.)	A.D., responsabile di funzione	Corruzione tra privati; istigazione alla corruzione tra privati; ostacolo alle attività di vigilanza di pubbliche autorità; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione attiva o passiva; corruzione in atti giudiziari; induzione indebita a dare o promettere utilità; istigazione alla corruzione; induzione indebita a dare o promettere utilità, corruzione attiva e passiva, corruzione in atti giudiziari, istigazione alla corruzione - di membri degli organi UE o di funzionari UE; traffico di influenze illecite; omicidio o lesioni gravi e gravissime aggravati dalla violazione delle norme sulla prevenzione degli infortuni sul lavoro e delle malattie professionali	**RISCHIO DIRETTO:** **Art. 25-ter d.lgs 231/2001 (artt 2635, 2635-bis, 2638 c.c.)** **RISCHIO STRUMENTALE:** **Art. 25 d.lgs 231/2001;** **Art. 25-septies d.lgs 231/2001**
Valutazione dell'andamento dei contratti attivi e passivi con gli utilizzatori della rete rispetto agli obiettivi fissati nel Piano Industriale	Responsabile di funzione	Corruzione tra privati; istigazione alla corruzione tra privati; ostacolo alle attività di vigilanza di pubbliche autorità; malversazione di beni pubblici; indebita percezione di erogazioni pubbliche; truffe ai danni dello Stato; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione attiva o passiva; corruzione in atti giudiziari; induzione indebita a dare o promettere utilità; istigazione alla corruzione; induzione indebita a dare o promettere utilità, corruzione attiva e passiva, corruzione in	**RISCHIO DIRETTO:** **Art. 25-ter d.lgs 231/2001 (artt 2635, 2635-bis, 2638 c.c.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 640, 640-bis c.p.);** **Art. 25 d.lgs 231/2001**

		atti giudiziari, istigazione alla corruzione - di membri degli organi UE o di funzionari UE; traffico di influenze illecite	
Recupero crediti (fase precontenziosa)	Responsabile di funzione, responsabile di funzione Affari legali Capogruppo	Malversazione di beni pubblici; indebita percezione di erogazioni pubbliche; truffe ai danni dello Stato; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione attiva o passiva; corruzione in atti giudiziari; induzione indebita a dare o promettere utilità; istigazione alla corruzione; induzione indebita a dare o promettere utilità, corruzione attiva e passiva, corruzione in atti giudiziari, istigazione alla corruzione - di membri degli organi UE o di funzionari UE; traffico di influenze illecite; corruzione tra privati; istigazione alla corruzione tra privati; ostacolo alle funzioni di vigilanza da parte di autorità pubbliche	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 640, 640-bis c.p.);** **Art. 25 d.lgs 231/2001;** **Art. 25-ter d.lgs 231/2001 (artt 2635, 2635-bis, c.c.)** **RISCHIO STRUMENTALE:** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2638 c.c.)**

III.1.2. ELEMENTI DI CONTROLLO.

III.1.2.1. Gestione ed esecuzione del processo di elaborazione del budget aziendale

Infratel Italia assicura correttezza, tempestività e trasparenza nella conduzione delle attività finalizzate alla formale definizione delle linee guida per la formazione del budget, per l'elaborazione periodica dei consuntivi e delle previsioni della Società.

L'Ufficio Controllo di Gestione assicura il processo periodico di pianificazione del budget, nel rispetto degli indirizzi stabiliti dall'Amministratore Delegato e sulla base delle tempistiche comunicate dalla Capogruppo, ed è tenuto a comunicare alle funzioni aziendali interessate, ovvero alle funzioni titolari di budget, le tempistiche e le modalità per la redazione del budget di pertinenza, con congruo anticipo.

Ciascuna funzione titolare di budget è tenuta, nel rispetto delle tempistiche e delle modalità stabilite, alla comunicazione del budget di pertinenza elaborato in collaborazione con le funzioni interne competenti, che dovrà indicare:

- il valore dei ricavi di commessa/progetto previsto per il periodo di riferimento sulla base delle convenzioni già attive e delle opportunità commerciali che possono essere perfezionate nel periodo di riferimento, come stimato di concerto con le funzioni competenti;
- il fabbisogno delle risorse complessive, professionali ed infrastrutturali, necessarie alla realizzazione delle attività di commessa/progetto interna ed esterna di competenza e dei relativi dati economico-finanziari.

L'Ufficio Controllo di Gestione giunge all'elaborazione del budget complessivo della Società, verificando e rettificando le informazioni ricevute da ciascuna funzione interessata anche sulla base delle informazioni presenti nella contabilità di Amministrazione. **Il budget viene sottoposto, previo riscontro da parte delle funzioni competenti di Capogruppo, ad approvazione dell'Amministratore Delegato e del Consiglio di Amministrazione. Eventuali variazioni inerenti al budget, al preconsuntivo e alle previsioni sono comunicate dall'Ufficio Controllo di Gestione alle funzioni interessate.**

III.1.2.2. Monitoraggio e recupero crediti verso committenti e operatori terzi. Verifica dello scadenzario delle fatture emesse dall'Ufficio Amministrazione verso il Ministero

Relativamente alla gestione dei crediti aziendali, al fine di assicurare adeguata e tempestiva informazione circa le previsioni di incasso, l'insorgenza di morosità e lo stato delle procedure di recupero di eventuali crediti scaduti, Infratel Italia garantisce che il processo di gestione dei crediti sia condotto in maniera corretta, trasparente e tracciabile, attraverso lo svolgimento delle seguenti attività:

- il monitoraggio dei **crediti** scaduti sulla base della situazione contabile dei debitori rilevata dall'Ufficio Amministrazione, che è tenuto alla corretta imputazione e alla tempestiva registrazione delle singole partite di credito e dei relativi incassi;
- la **predisposizione periodica della reportistica dei crediti scaduti** oggetto di comunicazione alle funzioni interessate anche al fine di ottenere indicazioni relative alle possibili cause;
- la **gestione delle problematiche relative al mancato incasso** di ciascun credito alla sua scadenza, che viene condivisa con gli Uffici titolati della Società, attraverso **l'emissione di una o più comunicazioni formali di sollecito**. **Dopo il parere dell'Ufficio interessato e dell'Ufficio Affari Legali presso la Capogruppo**, **vengono attuate le seguenti possibili soluzioni alternative, previa verbalizzazione delle motivazioni alla base dell'azione stabilita, da sottoporre all'Amministratore Delegato per approvazione**: la definizione di piani di rientro e/o consolidamento del credito; il ricorso al recupero coattivo; la cancellazione dei crediti per i quali le azioni legali non risultino economicamente convenienti;
- **nel caso di recupero coattivo del credito, la comunicazione formale all'Ufficio Affari Legali presso la Capogruppo di tutta la documentazione pertinente** attestante la posizione creditoria e le azioni già poste in essere per il recupero del credito.

L'Ufficio Affari Legali presso la Capogruppo assicura la predisposizione e la comunicazione formale delle lettere di diffida ai soggetti debitori nonché, qualora necessario, l'attivazione della procedura di gestione del contenzioso; emette inoltre una **comunicazione semestrale e all'Ufficio Amministrazione e Bilancio presso la Capogruppo contenente una situazione riepilogativa dei crediti in contenzioso**, l'indicazione dei soggetti coinvolti, della natura e dell'importo, del tipo di azione intrapresa e del relativo stato, delle possibilità di recupero del credito.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate all'Organismo di Vigilanza e al RPCT, l'Ufficio Controllo di Gestione è tenuto alla comunicazione periodica, su base semestrale, all'Organismo di Vigilanza di un'informativa riepilogativa dei crediti scaduti.

III.1.2.3. Controlling e reporting direzionale, tramite elaborazione di previsioni, consuntivi, analisi di flow-chart e monitoraggio del livello di conseguimento degli obiettivi (es. KPI, indicatori di processo). Controllo dell'andamento economico della Società effettuato con l'analisi degli scostamenti

L'Ufficio Controllo di Gestione richiede periodicamente a ciascuna funzione interessata di elaborare la migliore stima dei nuovi valori economico-finanziari di competenza, indicando eventuali scostamenti rispetto a quanto precedentemente pianificato, sulla base dei dati di consuntivo disponibili e delle informazioni relative alle nuove opportunità o modifica di quelle correnti. Sulla base dei dati previsionali ricevuti e delle informazioni di consuntivo disponibili, **l'Ufficio Controllo di Gestione è tenuto alla verifica periodica del rispetto del budget definito. Gli esiti di tale verifica sono sottoposti ad esame da parte dell'Amministratore Delegato quindi comunicati alle funzioni competenti di Capogruppo**.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate, l'Ufficio Controllo di Gestione è tenuto alla comunicazione tempestiva all'Organismo di Vigilanza, e

al RPCT, se di competenza, del budget annuale approvato e dei consuntivi e delle previsioni periodiche indicative di eventuali scostamenti e dei consuntivi indicanti l'analisi degli scostamenti e le deviazioni dal Budget.

In ogni caso, il responsabile dell'Ufficio Controllo di gestione, con cadenza almeno annuale, comunica all'OdV e al RPCT le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

III.1.2.4. Ulteriori attività di supporto gestionale e di controllo affidate alla funzione Controllo di Gestione

Tra le responsabilità dell'unità organizzativa Controllo di Gestione vi è quella della comunicazione dei dati di monitoraggio ad Invitalia S.p.A. in qualità di Capogruppo, rispetto alla quale viene svolta un'attività di raccolta ed aggregazione dei dati acquisiti in sede di monitoraggio dell'andamento generale della Società.
Nella mappatura dei rischi, tale attività risulta meramente strumentale in quanto consistente in un'attività di supporto, coordinamento e monitoraggio priva di significativa esposizione, in quanto funzionale al controllo di secondo e terzo livello della Capogruppo. Tuttavia, non si può escludere che una grave carenza nello svolgimento della stessa possa agevolare od occultare la commissione di un illecito, né, altresì, può escludersi che i responsabili di tale funzione partecipino in concorso con le funzioni coinvolte in altre ipotesi di rischio, divenendo in tal caso essi stessi direttamente autori dell'illecito.

Di seguito il riepilogo delle attività meramente strumentali:

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Comunicazione dati di monitoraggio alla capogruppo	A.D., responsabile di funzione	Falsità in documento pubblico informatico; false comunicazioni sociali; impedito controllo; ostacolo alle funzioni di vigilanza da parte di pubbliche autorità	**RISCHIO STRUMENTALE:** **Art. 24-bis d.lgs 231/2001 (art. 491-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2621, 2625, 2638 c.c.)**

Il *risk owner* di primo livello svolge le proprie attività in coordinamento con le altre funzioni interne e della Capogruppo coinvolte, avendo come ulteriori punti di attenzione le attività ed i rischi strumentali sopra indicati. Il process owner garantisce l'effettività e l'efficacia dei controlli, adeguando periodicamente le procedure. A tal fine richiede una informativa ai risk owner, sulla base della quale egli acquisisce le informazioni rilevanti per attuare le opportune azioni correttive e alimentare i flussi informativi, segnalando tempestivamente all'OdV, e al RPCT se di competenza, eventuali anomalie o non conformità riscontrate.

III.2 ACQUISTI, AFFARI GENERALI E DEMAND ORGANIZZAZIONE

III.2.1. ATTIVITÀ A RISCHIO E POTENZIALI REATI (ACQUISTI, AFFARI GENERALI E DEMAND ORGANIZZAZIONE)

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Coordinamento facility & building management	Responsabile di funzione	Falsità in documento pubblico informatico; accesso abusivo a sistema informatico; distruzione di beni culturali; riciclaggio di beni culturali	**RISCHIO DIRETTO:** **art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter c.p.);** **art. 25-septiesdecies d.lgs. 231/2001 (art. 518-duodecies c.p.);** **art. 25-duodevicies d.lgs 231/2001 (art. 518-sexies c.p.)**

III.2.2. ATTIVITÀ A RISCHIO E POTENZIALI REATI (ACQUISTI)

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001

RUP per affidamento diretto	RUP/Responsabile di funzione/referente contrattuale interno	Falsità in documento pubblico informatico; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; concussione, corruzione attiva o passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione tra privati; istigazione alla corruzione tra privati; riciclaggio e reimpiego di beni di provenienza illecita; omicidio colposo aggravato dalla violazione delle norme sulla prevenzione degli infortuni sul lavoro; lesioni gravi o gravissime aggravate dalla violazione delle norme sulla prevenzione degli infortuni sul lavoro; rifiuto d'atti d'ufficio. omissione malversazione di beni pubblici; frode in pubbliche forniture; truffe, anche informatiche, ai danni di PA centrali o locali; inquinamento ambientale; disastro ambientale; inquinamento e disastro ambientale colposi; uccisione di specie animali o vegetali protette; distruzione o deterioramento di habitat all'interno di un sito protetto; impiego di cittadini di paesi terzi irregolari; favoreggiamento della permanenza illegale dello straniero; uso nelle dichiarazioni relative alle imposte sui redditi o all'IVA di fatture oggettivamente o soggettivamente false; dichiarazione fraudolenta mediante altri raggiri; dichiarazione infedele o omessa per importi superiori alle soglie di punibilità; distruzione o occultamento di documenti contabili; sottrazione fraudolenta al pagamento di imposte compensazione indebita ai danni dell'UE; falsificazione in scrittura privata relativa a beni culturali; esportazione illecita di beni culturali; distruzione di beni culturali; riciclaggio di beni culturali	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (art. 491-bis c.p.);** **Art. 25 d.lgs. 231/2001 (ad eccezione artt. 319-ter e 322-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis c.c.);** **Art. 25-octies d.lgs. 231/2001 (art. 648-bis, 648-ter c.p.);** **Art. 25-septies d.lgs 231/2001** **L. 190/2012 - 328, c.p.** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (Artt. 316-bis, 356, 640, 640-bis, 640-ter, c.p.);** **Art. 25-undecies d.lgs 231/2001 (artt. 452 bis, 452-quater, 452-quinquies, 727-bis, 733-bis c.p.);** **Art. 25-duodecies;** **Art. 25-quinquiesdecies d.lgs. 231/2001 (art. 2, 3, 4, 5, 10, 10-quater, 11 d.lgs. 74/2000);** **Art. 25-septiesdecies d.lgs. 231/2001 (artt.** **518-octies, 518-undecies; 518-duodecies c.p.);** **Art. 25-duodevicies d.lgs. 231/2001 (art. 518-sexies, c.p.)**
Acquisti (lavori, servizi, forniture) per importi inferiori alle soglie di affidamento diretto	A.D., responsabile di funzione	Malversazione di fondi pubblici; percezione indebita di erogazioni pubbliche; turbata libertà degli incanti; turbata libertà del processo di scelta del contraente; frode nelle pubbliche forniture; truffe, anche informatiche, ai danni di PA centrali o locali; peculato, peculato mediante profitto dell'errore altrui e indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; concussione; corruzione attiva o passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione tra privati; istigazione alla corruzione tra privati; riciclaggio; reimpiego di beni di provenienza illecita; falsità in documento pubblico informatico; accesso abusivo a sistema informatico; danneggiamento di dati o programmi informatici; anche di interesse pubblico; uso nelle dichiarazioni relative alle imposte sui redditi o all'IVA di fatture oggettivamente o soggettivamente false; dichiarazione fraudolenta mediante altri raggiri	**RISCHIO DIRETTO:** **Art. 24 d.lgs. 231/2001;** **Art. 25 d. lgs. 231/2001 (ad eccezione artt. 319-ter e 322-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis c.c.);** **Art. 25 octies (artt. 648-bis, 648-ter cp)** **RISCHIO STRUMENTALE:** **Art. 24-bis d.lgs. 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.).** **Art. 25 quinquiesdecies d.lgs. 231/2001 (artt. 2, 3 d.lgs. 74/2000)**
Selezione, contrattualizzazione e gestione dei fornitori	A.D., responsabile di funzione, referente contrattuale interno	Malversazione di fondi pubblici; percezione indebita di erogazioni pubbliche; turbata libertà degli incanti; turbata libertà del processo di scelta del contraente; frode nelle pubbliche forniture; truffe, anche informatiche, ai danni di PA centrali o locali; concussione, corruzione attiva o passiva; induzione indebita a dare o promettere utilità; traffico di influenze illecite; corruzione tra privati; istigazione alla corruzione tra privati; riciclaggio; reimpiego di beni di provenienza illecita; falsità in documento pubblico informatico; accesso abusivo a sistema informatico; danneggiamento di dati o programmi informatici, anche di interesse pubblico; uso nelle dichiarazioni relative alle imposte sui redditi o all'IVA di fatture oggettivamente o soggettivamente false; dichiarazione fraudolenta mediante altri raggiri	**RISCHIO DIRETTO:** **Art. 24 d.lgs. 231/2001;** **Art. 25 d. lgs. 231/2001 (artt. 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (art. 2635, 2635-bis c.c.);** **Art. 25 octies (artt. 648-bis, 648-ter cp)** **RISCHIO STRUMENTALE:** **Art. 24-bis d.lgs. 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.).** **Art. 25 quinquiesdecies d.lgs. 231/2001 (artt. 2, 3 d.lgs. 74/2000)**

Gestione dei processi di e-procurement	A.D., responsabile di funzione	Malversazione di fondi pubblici; percezione indebita di erogazioni pubbliche; turbata libertà degli incanti; turbata libertà del processo di scelta del contraente; frode nelle pubbliche forniture; truffe, anche informatiche, ai danni di PA centrali o locali; falsità in documento pubblico informatico; accesso abusivo a sistema informatico; danneggiamento di dati o programmi informatici; corruzione attiva o passiva, induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite rifiuto d'atti d'ufficio. omissione	**RISCHIO DIRETTO:** **Art. 24 d.lgs. 231/2001;** **Art. 24-bis d.lgs. 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.);** **Art. 25 d. lgs. 231/2001 (artt. 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.)** **L. 190/2012 (art. 328 c.p.)** **RISCHIO STRUMENTALE:** **Art. 25 d. lgs. 231/2001 (ad eccezione artt. 317, 319-ter e 322-bis c.p.)**
Definizione dei fabbisogni aziendali	A.D., responsabile di funzione, funzioni richiedenti	Falsità in documento pubblico informatico; accesso abusivo a sistema informatico; danneggiamento di dati o programmi informatici; anche di interesse pubblico; false comunicazioni sociali; ostacolo al controllo dei soci o degli organi sociali; restituzione indebita di conferimenti ai soci; ripartizione illegale degli utili; operazioni illecite su azioni o quote sociali; operazioni dolose in danno dei creditori; formazione fittizia del capitale; corruzione tra privati; determinazione fraudolenta della maggioranza assembleare; aggiotaggio; ostacolo alle attività di vigilanza di pubbliche autorità; omicidio colposo aggravato dalla violazione delle norme sulla prevenzione degli infortuni sul lavoro; lesioni gravi o gravissime aggravate dalla violazione delle norme sulla prevenzione degli infortuni sul lavoro	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs. 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter, c.p.);** **Art. 25-ter d.lgs 231/2001** **RISCHIO STRUMENTALE:** **Art. 25-septies d.lgs. 231/2001**
Controllo relativo alla sussistenza e permanenza dei requisiti generali e speciali prescritti in capo agli affidatari	Responsabile di funzione	Falsità in documento pubblico informatico; accesso abusivo a sistema informatico; danneggiamento di dati o programmi informatici; corruzione attiva o passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite rifiuto d'atti d'ufficio. omissione	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter, c.p.);** **Art. 25 d. lgs. 231/2001 (artt. 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.)** **L. 190/2012** **RISCHIO STRUMENTALE:** **Art. 25 d. lgs. 231/2001**

III.2.3. ATTIVITÀ A RISCHIO E POTENZIALI REATI (AFFARI GENERALI E DEMAND ORGANIZZAZIONE)

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Gestione del parco auto aziendale e attività di «mobility management»	Responsabile di funzione/funzioni coinvolte	Malversazione di fondi pubblici; percezione indebita di erogazioni pubbliche; turbata libertà degli incanti; turbata libertà del processo di scelta del contraente; frode nelle pubbliche forniture; truffe, anche informatiche, ai danni di PA centrali o locali; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; ricettazione; riciclaggio; reimpiego in attività produttive o autoriciclaggio di beni di provenienza illecita; concussione, corruzione attiva o passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione e istigazione alla corruzione tra privati	**RISCHIO DIRETTO:** **Art. 24 d.lgs. 231/2001;** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis e 316 c.p.);** **Art. 25-octies d.lgs 231/2001** **RISCHIO STRUMENTALE:** **Art. 25 d. lgs. 231/2001 (artt. 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (art. 2635, 2635-bis c.c.)**

Gestione dei servizi generali, di facility management, space planning e controllo delle relative forniture	Responsabile di funzione	Malversazione di fondi pubblici; percezione indebita di erogazioni pubbliche; turbata libertà degli incanti; turbata libertà del processo di scelta del contraente; frode nelle pubbliche forniture; truffe, anche informatiche, ai danni di PA centrali o locali; peculato, peculato mediante profitto dell'errore altrui e indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione e istigazione alla corruzione tra privati; ricettazione; riciclaggio; reimpiego in attività produttive o autoriciclaggio di beni di provenienza illecita sottrazione o danneggiamento di cose sottoposte a sequestro; Violazione colposa di doveri inerenti alla custodia	**RISCHIO DIRETTO:** **Art. 24 d.lgs. 231/2001;** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25 ter D .Lgs 231/2001 (artt. 2635, 2635-bis c.c.);** **Art. 25-octies d.lgs 231/2001** **L- 190/2012 (334, 335 c.p.)** **RISCHIO STRUMENTALE:** **Art. 25 d. lgs. 231/2001 (art. 318, 319, 319-quater c.p.);** **Art. 25-ter d.lgs 231/2001 (art. 2635 c.c.). 2635 c.c.)**
Gestione sistema del protocollo informatico	Responsabile di funzione/segreteria	Falsità in documento pubblico informatico; accesso abusivo a sistema informatico	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs. 231/2001 (artt. 491-bis, 615-ter c.p.)** **RISCHIO STRUMENTALE:** **OCCULTAMENTO TRACCE ILLECITI GIA' CONSUMATI**
Dematerializzazione dell'archivio aziendale	Responsabile di funzione, segreteria, responsabile funzione coinvolta	Falsità in documento pubblico informatico; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs. 231/2001 (art. 491-bis c.p.)** **RISCHIO STRUMENTALE:** **Art. 25-ter d.lgs. (art. 2638 c.c.)**

III.2.4. ELEMENTI DI CONTROLLO

III.2.4.1. Acquisti (lavori, servizi, forniture) per importi inferiori alle soglie di affidamento diretto. Selezione, contrattualizzazione e gestione dei fornitori. Definizione dei fabbisogni aziendali. Controllo relativo alla sussistenza e permanenza dei requisiti generali e speciali prescritti in capo agli affidatari.

Infratel Italia assicura la pianificazione degli acquisti su base annuale, in accordo con gli elementi di controllo definiti per il processo di budget: ciascuna **richiesta di acquisto** di beni/servizi/lavori, viene infatti sottoposta all'**approvazione del titolare di budget** e della funzione Controllo di Gestione per la verifica della corretta imputazione della spesa con il budget di Ufficio e la Commessa di riferimento.
La richiesta di acquisto deve contenere una nota motivazionale che definisca ragioni e finalità relative alla commessa interna o esterna di riferimento e, ove applicabile, una descrizione dei beni e servizi richiesti, che consentano di individuare le specifiche tecniche di acquisto. Qualora una richiesta di acquisto non sia presente nel budget degli acquisti, o non sia capiente il budget dell'Ufficio, la stessa deve essere sottoposta ad **approvazione da parte dei Soggetti titolati di Infratel Italia.**
Tale iter procedurale è svolto affinché Infratel Italia possa assicurare che l'acquisizione di lavori, servizi e forniture avvenga nel rispetto dei principi di efficacia, efficienza ed economicità dell'azione amministrativa, oltre che dei principi di libera concorrenza, non discriminazione, proporzionalità e parità di trattamento.

Infratel Italia seleziona gli operatori economici con i quali instaurare rapporti di fornitura di beni e servizi, mediante l'**Albo interno o quello istituito presso la Capogruppo**. Qualora all'esito della ricerca non risultino fornitori idonei o disponibili a rendere la prestazione richiesta, l'Ufficio Affari Generali, Acquisti e Demand Organizzazione avvierà il processo di selezione di ulteriori fornitori attraverso ricerche di mercato. Una volta identificato il fornitore e verificata la sua disponibilità a fornire i beni e servizi richiesti, l'Ufficio chiederà al fornitore selezionato di iscriversi all'Albo.

Gli uffici competenti della Capogruppo, nel rispetto della normativa vigente in materia di appalti pubblici,

assicurano:

- la definizione e il tempestivo **aggiornamento dei requisiti di ammissibilità in Albo** degli operatori economici e degli studi legali, nonché l'elenco della **documentazione che ne attesti il possesso**. Tra i requisiti di ammissibilità dovranno essere considerati l'area di competenza, la qualifica professionale, l'esperienza, nonché l'affidabilità ed onorabilità del contraente, anche in relazione alle disposizioni normative vigenti in materia di anticorruzione;
- **la cancellazione dall'Albo**, in caso di cessazione dell'attività, perdita dei requisiti di ammissibilità, gravi inadempimenti contrattuali. Gli studi legali sono sottoposti a valutazione anche in relazione al raggiungimento di opportuni livelli di servizio, preliminarmente stabiliti ed oggetto di riscontro da parte delle funzioni interessate dai servizi erogati.

L'Ufficio Acquisti, Affari Generali e Demand Organizzazione assicura l'affidamento di lavori, servizi e forniture agli operatori economici e professionisti iscritti all'Albo, ovvero in possesso dei suddetti requisiti, ad eccezione **di spese occasionali e di modesto importo**[16] per le quali Infratel Italia si riserva di procedere con l'acquisto anche tramite fornitori non in Albo.

Inoltre, ove previsto dalle norme, al fine di assicurare la qualificazione dei fornitori e la qualità dei servizi prestati/forniture effettuate, e comunque in base alla tipologia di servizi da affidare, l'Ufficio Affari Generali, Acquisti e Demand Organizzazione procede con l'individuazione degli operatori economici anche tramite:

- portale PA (piattaforma dedicata alla Pubblica Amministrazione, raggiungibile all'indirizzo web www.acquistinretepa.it);
- elenchi professionali riconosciuti (es. elenco nazionale archeologi professionisti del Ministero della Cultura, ordini professionali, etc.).

Per quel che concerne la redazione degli atti/contratti, l'unità Legale e Controllo Operativo PNRR, in coordinamento con la funzione Affari Legali presso la Capogruppo, ove di competenza, verifica gli elementi essenziali dello strumento negoziale, e si accerta della presenza di specifiche clausole di risoluzione da applicarsi ai contratti di fornitura, attivabili in caso di inosservanza o violazione del Codice Etico e delle previsioni del Modello 231, Parte Generale e Parte Speciale, e del Piano di Prevenzione della Corruzione, nonché di eventuali regole operative imposte al fornitore e necessarie per l'espletamento della prestazione. Tali clausole risolutive sono utilizzate anche qualora la controparte si renda inadempiente agli obblighi contrattuali, o vengano meno i presupposti di legittimità della prestazione contrattualizzata, per la perdita dei requisiti soggettivi necessari al corretto espletamento delle obbligazioni assunte[17].

In sede di stipula del contratto, la controparte è tenuta a fornire un'**apposita dichiarazione** circa l'assenza di condanne con sentenza passata in giudicato, o provvedimenti equiparati in procedimenti giudiziari relativi ai reati contemplati dal D.Lgs. 231/01. Per quanto di rilievo in materia di contratti pubblici, la controparte dovrà altresì fornire le dichiarazioni necessarie al fine delle verifiche dei requisiti generali e speciali richiesti dalla normativa, nonché dell'assenza di cause di esclusione o decadenza.
Nei contratti aventi ad oggetto l'**acquisizione di prodotti, tutelati da diritti di proprietà industriale**, è richiesta la presenza di **specifiche clausole** con cui la controparte attesti:

- **di essere il legittimo titolare dei diritti** di sfruttamento economico sui marchi, brevetti, segni distintivi, disegni o modelli oggetto di cessione, o comunque di aver ottenuto dai legittimi titolari l'autorizzazione alla loro concessione in uso a terzi;
- che i marchi, brevetti, segni distintivi, disegni o modelli oggetto di cessione, o di concessione in uso,

[16] Prestabilito nell'ambito di procedure/istruzioni interne

[17] Devono essere inoltre prestabiliti i termini massimi entro i quali il fornitore inadempiente deve essere estromesso dal Contratto

non violano alcun diritto di proprietà industriale in capo a terzi;

- **l'impegno a preservare la Società da qualsivoglia danno o pregiudizio** per effetto della non veridicità, inesattezza o incompletezza di tale dichiarazione.

Inoltre, sono svolte verifiche sulla provenienza dei beni, in particolar modo quando si tratta di beni non nuovi, previa acquisizione di un certificato che ne attesti la provenienza lecita.

Gli **affidamenti dei singoli incarichi** ad operatori economici/consulenti (legali, fiscali, tributarie, etc..) possono essere disciplinati **mediante** diverse modalità, tra cui gli **Accordi Quadro**, che sono sottoposti all'**autorizzazione dei Soggetti titolati** della Società e prevedono una **richiesta formale presentata all'Ufficio Affari generali, Acquisti e Demand Organizzazione,** che indichi le esigenze, i possibili operatori candidati a seguire l'attività e le motivazioni che sottendono il loro suggerimento (tra cui area di competenza, esperienza pregressa, continuità di azione).

I **Soggetti titolati della Società stabiliscono i limiti di importo applicabili** ai singoli Accordi e i criteri attraverso i quali valutare la **congruità delle tariffe** applicabili a ciascun Accordo Quadro, tra cui l'aderenza rispetto agli standard di mercato ed alle eventuali disposizioni legislative applicabili.

Il titolare del budget, come individuato nell'ambito del Controllo di Gestione, individua il referente di contratto tra coloro che hanno le competenze per controllare la corretta esecuzione della fornitura/prestazione. Nel caso di **fornitura di beni, il referente verifica** la rispondenza del mittente e di quanto ricevuto rispetto a quanto ordinato, nonché la sussistenza di documentazione attestante la provenienza e la liceità dei prodotti; nel caso di **prestazione di servizi**, **il referente di contratto verifica** la regolarità della prestazione, tramite l'accertamento del rispetto dei termini contrattuali.

Il referente di contratto, inoltre, effettua le seguenti attività:

- l'invio di un'eventuale **contestazione formale al fornitore**, nel caso di eventuali **inadempimenti rilevati** durante il rapporto di fornitura, per il tramite dei soggetti preposti ed in accordo con il titolare di budget e l'Ufficio Legale presso la Capogruppo;

- **la verifica degli importi della fattura passiva, rispetto ai requisiti contrattuali ed in relazione alle evidenze della prestazione/fornitura erogata**. Qualora quest'ultima non rispetti i requisiti - consultando l'unità Legale e Controllo operativo PNRR, in coordinamento con Affari Legali della Capogruppo, per quanto di competenza, e il titolare di budget - anche per il tramite degli Uffici competenti, provvede all'adozione di **opportune azioni correttive da sottoporre ad approvazione dell'Amministratore Delegato e/o dei Soggetti titolati della Società**.

Nel caso di **consulenze/collaborazioni fornite da persone fisiche**[18], l'Ufficio Acquisti, Affari Generali e Demand Organizzazione, in collaborazione con gli Uffici interni competenti, assicura:

- che sia **formalizzata da parte dell'Ufficio richiedente**, anche tramite **una richiesta di acquisto**, l'esigenza di ricorrere a collaboratori/consulenti esterni, o che sia **attuato l'iter autorizzativo da parte del Responsabile dell'Ufficio richiedente e dei Soggetti titolati della Società**[19];
- che il **processo di ricerca e selezione del consulente/collaboratore** avvenga coinvolgendo l'Ufficio richiedente e altri soggetti interni identificati dall'Amministratore Delegato, **attraverso il confronto di più soggetti candidati idonei, rispetto ai requisiti richiesti** dall'Ufficio richiedente e sulla base di una valutazione condivisa delle loro capacità tecnico-professionali;

[18] Assegnazione di incarichi specialistici in situazioni di necessità di natura tecnica/operativa non rientranti negli incarichi di collaborazione ex art. 7 comma 6 del D.Lgs. 165/2001 gestiti dalla Capogruppo

[19] In base ai poteri conferiti dal sistema di procure e deleghe aziendali

- che la **proposta economico contrattuale sia congrua** rispetto ai riferimenti di mercato;
- che siano **accertati e valutati - anche mediante autocertificazione - i rapporti, diretti o indiretti, del candidato con soggetti della Pubblica Amministrazione,** o facenti capo ai fornitori/partner di Infratel Italia;
- la **verifica di affidabilità/onorabilità del candidato, attraverso l'esame di atti e documenti attestanti tali requisiti** (tra cui carichi pendenti e casellario giudiziario), ovvero la **sottoscrizione di un'autodichiarazione** da parte dello stesso ai sensi della normativa vigente, circa il possesso dei suddetti requisiti;
- **nell'ambito della gestione dei rapporti con la Pubblica Amministrazione**, l'applicazione di opportuni **meccanismi di verifica**, anche mediante autodichiarazione del candidato, che non siano in essere **collaborazioni relative allo stesso oggetto con le medesime amministrazioni pubbliche, ai sensi della normativa vigente in materia di Anticorruzione**;
- la presenza, nel contratto di collaborazione/consulenza, di opportune clausole di risoluzione in caso di inosservanza o violazione del Codice Etico e delle previsioni del Modello 231, Parte Generale e Parte Speciale, nonché di eventuali regole operative imposte nell'espletamento della prestazione. L'Ufficio Acquisti assicura la ricezione e la presa visione da parte del collaboratore/consulente delle norme contenute nei suddetti documenti, anche attraverso la consegna della copia controfirmata;
- la richiesta del **conto corrente dedicato** ai sensi della normativa vigente;
- che i **documenti/lettere/atti formali,** preordinati alla collaborazione/consulenza, siano **firmati dai Soggetti titolati, dotati di specifica procura o delega** in materia, nonché dalla risorsa interessata;
- **qualora** - nel caso sia richiesta una **specializzazione tale che** l'attività possa essere svolta solo da un numero ristretto di specialisti, o da una singola persona fisica - **sia necessario conferire un incarico professionale ad uno specifico soggetto, l'Ufficio Acquisti in aggiunta alle suddette determinazioni assicura che siano verbalizzate, da parte dell'Ufficio richiedente, le motivazioni per le quali è necessario ricorrere a tale soggetto, segnalando al Presidente/Amministratore Delegato la sussistenza di incarichi ripetuti allo stesso soggetto**.

Negli affidamenti di lavori o servizi per manutenzione o restauro dei beni aziendali sottoposti a vincoli da parte del Ministero dei beni culturali sono rispettate tutte le cautele necessarie ad impedire il danneggiamento o l'asportazione di essi. L'unità Acquisti, Affari Generali e Demand Organizzazione provvede all'inventariazione dei predetti beni. Nessun lavoro può essere eseguito su di essi in assenza delle prescritte autorizzazioni. Nei contratti per i predetti lavori o servizi sono predisposte specifiche clausole 231 per il rispetto delle procedure in materia.
La procedura per gli incarichi di collaborazione e l'acquisizione di prestazioni professionali è distinta da quella per gli acquisti.

Le procedure relative agli acquisti si conformano alle *policy* della Capogruppo, delle cui procedure Infratel Italia si avvale per esigenze specifiche, in base agli accordi contrattuali per i servizi da questa forniti. Per gli acquisti di valore superiore alle soglie previste per l'affidamento diretto, si osservano i principi indicati in ambito gare, e alle relative procedure organizzative.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate all'OdV, l'Ufficio Acquisti, Affari Generali e Demand Organizzazione è tenuto alla comunicazione periodica, su base annuale, di un'informativa riepilogativa degli acquisti/incarichi effettuati, indicativa dell'importo, del fornitore/consulente/collaboratore, della commessa interna/esterna di riferimento, della tipologia di fornitura, della procedura di affidamento/incarico utilizzata, comprensiva delle eventuali motivazioni extra budget e di urgenza, nonché dei fornitori/consulenti/collaboratori suggeriti dal committente e/o segnalati dalla funzione richiedente, allegando in tal caso il contenuto della relativa nota motivazionale. Comunica tempestivamente le criticità inerenti le richieste extra-budget.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate all'OdV e al RPCT, l'Ufficio Acquisti, Affari Generali e Demand Organizzazione è tenuto alla

comunicazione periodica, su base semestrale, di un'informativa riepilogativa dei controlli effettuati in capo agli affidatari e delle eventuali cause ostative alla permanenza riscontrate, nonché dei fornitori/consulenti/collaboratori suggeriti dal committente e/o segnalati dalla funzione richiedente, allegando in tal caso il contenuto della relativa nota motivazionale. Comunica tempestivamente le criticità inerenti la cancellazione dall'albo in caso di perdita dei requisiti per fatto illecito dei fornitori/consulenti/collaboratori.

In ogni caso, il responsabile dell'Ufficio Acquisiti, Affari Generali e Demand Organizzazione comunica all'OdV e al RPCT, con cadenza almeno annuale, le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

- *Funzione di Rup. Gestione della piattaforma di e-procurement.*

L'unità Acquisiti, Affari Generali e Demand Organizzazione predispone la nomina del RUP da sottoporre al dirigente preposto, secondo le deleghe e le procure vigenti, verificando i requisiti di competenza e onorabilità del soggetto da nominare ai sensi della normativa vigente, cui vanno allegati:

- un'autodichiarazione sull'assenza di conflitto di interessi;
- un modulo che il RUP dovrà compilare al termine della prestazione/fornitura ricevuta, per valutarne l'idoneità.

In attuazione dell'ecosistema nazionale di approvvigionamento digitale (e-Procurement) – ai sensi dell'art. 19 e ss., Parte II, D.lgs. 36/2023 la funzione Acquisti, Affari Generali e Demand Organizzazione cura la transizione verso la digitalizzazione del ciclo di vita dei contratti pubblici (articolato in programmazione, progettazione, affidamento ed esecuzione), nonché l'attuazione dell'ecosistema nazionale di approvvigionamento digitale (e-Procurement).

In particolare, cura gli adempimenti, l'inserimento dei dati e provvedere a chiedere gli adeguamenti, anche di tipo tecnico, necessari in vista della piena interoperabilità della Banca dati nazionale dei contratti pubblici (BDNCP) con le piattaforme di approvvigionamento digitale in uso alle stazioni appaltanti (ex art. 25 d.lgs. n. 36/2023), con il portale dei soggetti aggregatori e con la Piattaforma Digitale Nazionale Dati (PDND). Si rinvia per le ulteriori specifiche misure agli elementi di controllo indicati in Pianificazione, Gare e Ingegneria, paragrafo "Gestione dei procedimenti di affidamento per il rispetto di adempimenti normativi e del sistema di e-procurement".

III.2.4.2. *Gestione dei servizi generali, di facility management, space planning e controllo delle relative forniture*

L'unità Affari Generali e Demand Organizzazione è responsabile, sotto il coordinamento dell'unità Acquisti, Affari Generali e Demand Organizzazione, della gestione degli asset e dei contratti delle relative forniture per tutti i servizi generali di Infratel Italia. Si rinvia, per quanto di interesse per la gestione degli *asset* della Società, alle misure generali indicate nel paragrafo *Gestione degli asset aziendali*.

III.2.4.3. *Gestione del parco auto aziendale e attività di «mobility management».*

L'unità **Affari Generali e Demand organizzazione** è responsabile della gestione del parco auto e motocicli aziendale, di proprietà o comunque nella disponibilità di Infratel Italia, che avviene nel rispetto dei principi di trasparenza ed imparzialità in fase di assegnazione, nonché di massima sicurezza esigibile in fase di manutenzione dei veicoli. Inoltre, l'uso dei veicoli è regolato in modo da garantire la conformità agli scopi dell'ente. E' vietato appropriarsi dei veicoli aziendali o utilizzarli in maniera non conforme all'uso regolato dalle istruzioni operative. Le istruzioni operative indicano le necessarie verifiche di sicurezza da svolgere prima dell'avvio su tutti i mezzi, anche personali dei dipendenti, nell'esercizio del proprio ufficio. L'uso dei veicoli è censito e monitorato.

III.2.4.4. Gestione del Protocollo Informatico e Coordinamento del "Sistema Documentale Aziendale"

Per gli elementi di controllo relativi a questo processo vale quanto indicato nel paragrafo relativo alla Documentabilità e alla Tracciabilità e delle misure specifiche per la gestione dei sistemi informativi.

III.2.4.5. Dematerializzazione dell'archivio aziendale.

L'unità **Affari Generali e Demand Organizzazione** cura l'attività di dematerializzazione dell'archivio aziendale secondo principi di trasparenza, completezza e tempestività, garantendo la digitalizzazione della documentazione cartacea e la corrispondenza all'originale delle copie digitali acquisite. Cura inoltre la gestione dell'archivio aziendale, assicurando la conservazione ordinata della documentazione formata o ricevuta e l'individuabilità di singoli file. Si rinvia inoltre agli elementi di controllo generali per documentabilità e tracciabilità, nonché ai protocolli specifici per la gestione dei sistemi informativi.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate all'OdV e al RPCT, l'Ufficio Affari Generali e Demand Organizzazione trasmette annualmente una informativa relativa all'invio di report degli eventuali furti/smarrimenti/danneggiamenti degli asset aziendali, degli esiti dei controlli effettuati sul parco auto aziendale, dei mutamenti relativi alle sedi e ai servizi generali, delle verifiche sul fabbisogno di formazione, nonché degli eventuali smarrimenti/rimozioni dei documenti con l'indicazione di eventuali criticità aperte. Comunica tempestivamente le notizie di illeciti commessi sui beni aziendali. In caso negativo, attesta, con la medesima frequenza, l'assenza di eventi critici.

III.2.4.6. Ulteriori attività di supporto e di controllo affidate alla funzione Acquisti, Affari Generali e Demand Organizzazione.

Tra le responsabilità dell'unità organizzativa Acquisti, Affari Generali e Demand Organizzazione vi sono quelle del supporto organizzativo e operativo al vertice (ambito Affari generali), la verifica dell'assetto organizzativo e del dimensionamento della Società, la definizione ed individuazione dei ruoli aziendali e dei contratti, il presidio dei contratti di service e il coordinamento delle attività di compliance 231 (ambito Demand Organizzazione).
Nella mappatura dei rischi tali attività risultano meramente strumentali, in quanto consistono in attività di supporto, coordinamento e monitoraggio prive di un significativo margine di esposizione, funzionali al livello di controllo. Tuttavia, non si può escludere che una grave carenza nel loro svolgimento possa agevolare od occultare la commissione di un illecito, né, altresì, può escludersi che i responsabili di tali funzioni partecipino in concorso con le funzioni coinvolte in altre ipotesi di rischio, divenendo in tal caso essi stessi direttamente autori dell'illecito.
In particolare, la funzione Demand Organizzazione ha un ruolo strategico nella gestione della compliance 231 nel suo complesso, essendo responsabile del coordinamento delle relative attività.
Essa svolge inoltre tutte le attività di coordinamento correlate ai fabbisogni in termini di acquisti e di organizzazione, anche in relazione alle attività demandate in Service alla Capogruppo.
Di seguito il riepilogo delle attività meramente strumentali:

AREA	ATTIVITA' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
AFFARI GENERALI	Supporto organizzativo e operativo al vertice	Responsabile di funzione	Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza	**RISCHIO STRUMENTALE: art. 25-ter d.lgs 231/2001 (art. 2638 c.c.)**
DEMAND ORGANIZZAZIONE	Verifica ed adeguamento dell'assetto organizzativo e del dimensionamento della società	A.D.,CDA, Collegio sindacale/ responsabile di funzione, Referente Capogruppo,	Omicidio o lesioni gravi e gravissime aggravati dalla violazione delle norme sulla prevenzione degli infortuni sul lavoro e delle malattie professionali	**RISCHIO STRUMENTALE: Art. 25-septies d.lgs 231/2001**

	Definizione ed individuazione dei ruoli aziendali e dei contratti	A.D./ responsabile di funzione	Omicidio o lesioni gravi e gravissime aggravati dalla violazione delle norme sulla prevenzione degli infortuni sul lavoro e delle malattie professionali	**RISCHIO STRUMENTALE: Art. 25-septies d.lgs 231/2001**
	Coordinamento delle attività di compliance 231	Responsabile di funzione/consulenti esterni		**RISCHIO STRUMENTALE: TUTTI GLI ILLECITI NON PREVIAMENTE ESCLUSI DALLA MAPPATURA**
	Presidio contratti di service	Responsabile di funzione		**RISCHIO STRUMENTALE: TUTTI GLI ILLECITI REALIZZABILI NELLA GESTIONE DEI PROCESSI IN SERVICE**

Al fine di prevenire gli ulteriori rischi di illecito correlati a queste attività meramente strumentali, il *risk owner* di primo livello svolge la propria attività in coordinamento con le altre funzioni interne e della Capogruppo coinvolte, rispettando i principi generali di controllo e il codice etico, avendo come punti di attenzione i rischi strumentali sopra indicati.
Il process owner garantisce l'effettività e l'efficacia dei controlli, adeguando periodicamente le procedure. A tal fine richiede una informativa ai risk owner, sulla base della quale egli acquisisce le informazioni rilevanti per attuare le opportune azioni correttive e alimentare i flussi informativi, segnalando tempestivamente all'OdV, e al RPCT se di competenza, eventuali anomalie o non conformità riscontrate.

III.3 QUALITÀ, PRIVACY E SICUREZZA

III.3.1. ATTIVITÀ A RISCHIO E POTENZIALI REATI

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Gestione del SGSSL aziendale e attività inerenti la Certificazione UNI ISO 45001:2018.	A.D., responsabile di funzione, delegato ex art,. 16 TUSL, lavoratori	Omicidio o lesioni gravi e gravissime aggravati dalla violazione delle norme sulla prevenzione degli infortuni sul lavoro e delle malattie professionali; malversazione di erogazioni pubbliche; ricettazione; riciclaggio; reimpiego in attività produttive o autoriciclaggio di beni di provenienza illecita; uso nelle dichiarazioni relative alle imposte sui redditi o all'IVA di fatture oggettivamente o soggettivamente false; dichiarazione fraudolenta mediante altri raggiri; dichiarazione infedele o omessa per importi superiori alle soglie di punibilità; emissione di fatture oggettivamente o soggettivamente false; distruzione o occultamento di documenti contabili; compensazione indebita ai danni dell'UE; sottrazione fraudolenta alle procedure erariali di riscossione coattiva	**RISCHIO DIRETTO: Art. 25-septies d.lgs 231/2001** **RISCHIO STRUMENTALE: Art. 24 d.lgs. 231/2001 (art. 316-bis c.p.); Art. 25-octies d.lgs 231/2001; Art. 25-quinquiesdecies 231/2001**
Riesame della Politica, degli Obiettivi e delle attività di Formazione SSL.	A.D., Responsabile di funzione, RSPP, RSL, Preposti, Delegato ex art. 16 TUSL	Omicidio o lesioni gravi e gravissime aggravati dalla violazione delle norme sulla prevenzione degli infortuni sul lavoro e delle malattie professionali; malversazione di erogazioni pubbliche; ricettazione; riciclaggio; reimpiego in attività produttive o autoriciclaggio di beni di provenienza illecita; uso nelle dichiarazioni relative alle imposte sui redditi o all'IVA di fatture oggettivamente o soggettivamente false; dichiarazione fraudolenta mediante altri raggiri; dichiarazione infedele o omessa per importi superiori alle soglie di punibilità; emissione di fatture oggettivamente o soggettivamente false; distruzione o occultamento di documenti contabili; compensazione indebita ai danni dell'UE; sottrazione fraudolenta alle procedure erariale di riscossione coattiva	**RISCHIO DIRETTO: Art. 25-septies d.lgs 231/2001** **RISCHIO STRUMENTALE: Art. 24 d.lgs. 231/2001 (art. 316-bis c.p.); Art. 25-octies d.lgs 231/2001; Art. 25-quinquiesdecies 231/2001**

Gestione e implementazione del SGIQA e attività inerenti la Certificazione qualità UNI ISO 9001:2015.	A.D., Responsabile di funzione, Resp. SGIQA, Incaricato ambientale	Falsità in documento pubblico informatico; accesso abusivo a sistema informatico; danneggiamento di dati o programmi informatici anche di interesse pubblico; danneggiamento di sistemi informatici o telematici; inquinamento e disastro colposi in materia ambientale; attività organizzata per il traffico illecito di rifiuti; gestione non autorizzata di rifiuti; malversazione di beni pubblici; indebita percezione di erogazioni pubbliche; truffe, anche informatiche, ai danni di PA centrali o locali; ricettazione; riciclaggio; reimpiego in attività produttive o autoriciclaggio di beni di provenienza illecita	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter, 635-quater);** **Art. 25-undecies d.lgs 231/2001 (artt. 452-quinquies, 452-quaterdecies c.p./art. 260 d.lgs 152/2006; artt. 256, 257, d.lgs 152/2006)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs. 231/2001 (artt. 316-bis, 316-ter,** **640, 640-bis, 640-ter c.p.);** **art. 25-octies 231/2001**
Assistenza nei confronti dell'autorità giudiziaria a norma dell'art. 96 Codice delle comunicazioni elettroniche.	Responsabile di funzione	Falsità in documento pubblico informatico; omessa segnalazione all'Autorità giudiziaria o alla P.G. di condotte penalmente rilevanti ai sensi della L. n. 633/1941, degli artt. 615-ter e 640-ter c.p.; omessa comunicazione all'AGCOM di un punto di contatto diretto	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs. 231/2001 (art. 491-bis c.p.;** **art. 174-sexies l. 633/1941)**
Verifiche ispettive relative al SGSSL presso le sedi e i cantieri della società	Responsabile di funzione, Verifiche cantieri	Concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; corruzione e istigazione alla corruzione tra privati; omicidio o lesioni gravi e gravissime aggravati dalla violazione delle norme sulla prevenzione degli infortuni sul lavoro e delle malattie professionali; malversazione di beni pubblici; falsità in documento pubblico informatico; ricettazione; riciclaggio; reimpiego in attività produttive; autoriciclaggio di beni di provenienza di provenienza illecita; dichiarazione ai fini delle imposte dirette o dell'IVA fraudolente per uso di fatture oggettivamente o soggettivamente false, per altri artifici ovvero altrimenti infedeli	**RISCHIO DIRETTO:** **Art. 25 d.lgs 231/2001 (artt. 317, 318, 319, 319 quater, 320, 321, 322 c.p.);** **Art. 25-ter d.lgs 231/2001 (art. 2635 c.c.)** **Art. 25-septies d.lgs 231/2001** **RISCHIO STRUMENTALE:** **Art 24 d.lgs 231/2001 (art. 316-bis c.p.);** **Art. 24-bis d.lgs. 231/2001 (art. 491-bis c.p.);** **Art. 25-octies d.lgs 231/2001.** **Art. 25-quinquiesdecies d.lgs 231/2001 (art. 2, 3, d.lgs 74/2000)**

III.3.2. ELEMENTI DI CONTROLLO

L'Ufficio **Qualità, Privacy e Sicurezza** si occupa, in primo luogo, delle attività di gestione e controllo relative alla tutela della salute e sicurezza sui luoghi di lavoro e alla qualità ambientale.

III.3.2.1. Gestione della salute e sicurezza sui luoghi di lavoro

Per il coordinamento tra il MOGC 231 e il sistema di gestione della salute e sicurezza sui luoghi di lavoro di Infratel Italia vale quanto già delineato nel Capitolo I, cui si rinvia per la descrizione dei ruoli specifici e delle responsabilità all'interno del sistema di gestione SSL. L'unità organizzativa Privacy, Qualità e Sicurezza garantisce altresì i seguenti presidi di controllo:

III.3.2.2. *Pianificazione*

La politica di Infratel Italia, ovvero gli indirizzi e gli obiettivi generali che la Società si prefigge di raggiungere in materia di salute e sicurezza sul lavoro **è stabilita e comunicata dal Datore di lavoro**, a tutto il personale ed alle parti interessate. **La figura del Datore di lavoro coincide con l'Amministratore Delegato**, individuato con delibera del Consiglio di Amministrazione, tramite la quale gli sono conferiti adeguati poteri organizzativi e di spesa ai fini della tutela della salute e sicurezza sul lavoro del personale aziendale.

Il Datore di lavoro, anche per il tramite del Delegato del datore di lavoro, opera in collaborazione con il

Responsabile del servizio di prevenzione e protezione (RSPP), il Medico competente (MC) e il Responsabile dei lavori per la sicurezza (RLS), **in accordo alla normativa vigente,** e **assicura la valutazione documentata di tutti i rischi presenti nel perimetro della Società e nelle attività svolte dai lavoratori, nonché la definizione ed attuazione delle misure di prevenzione e protezione da adottare per eliminare o mitigare il più possibile i rischi evidenziati.**

Il Datore di Lavoro assicura inoltre, anche per il tramite degli incaricati - ciascuno per gli aspetti di competenza ed in accordo alla procura/delega/incarico conferiti - in collaborazione con il Responsabile del sistema di gestione, il RSPP e il MC:

- la definizione di un budget annuale specifico per la sicurezza sul lavoro;
- la definizione, per ogni funzione aziendale rilevante, di obiettivi e programmi di miglioramento dei livelli di salute e sicurezza dei lavoratori;
- l'identificazione, l'aggiornamento e il riesame periodico di tutte le previsioni normative applicabili alla Società in materia di sicurezza sul lavoro, quindi l'attuazione delle azioni necessarie al raggiungimento della conformità a dette previsioni.

Il **Datore di lavoro e/o suo delegato**, con il supporto degli incaricati per le attività di pertinenza, con riferimento ai singoli programmi, progetti o commesse implicanti la realizzazione di lavori per mezzo di cantieri temporanei o mobili ai sensi del titolo IV del D.Lgs. 81/01 e s.m.i., **assicurano**, anche attraverso la collaborazione delle funzioni aziendali competenti:

- la **verifica dell'idoneità tecnico-professionale** delle imprese e dei lavoratori autonomi operanti in cantiere;

- le **attività di vigilanza sull'operato dei soggetti nominati ai sensi di legge**, previa verifica del **possesso degli opportuni requisiti professionali definiti dalla normativa vigente**, quali il Responsabile lavori, il Coordinatore della sicurezza in fase di progettazione (CSP) ed in fase di esecuzione (CSE), con riferimento in particolare alla redazione, aggiornamento, riesame e comunicazione alle parti interessate (imprese appaltatrici ed esecutrici) del Piano di Sicurezza e Coordinamento (PSC) e del fascicolo tecnico, elaborati secondo le disposizioni normative vigenti, nonché alle attività di monitoraggio e verifica da parte di detti soggetti circa il rispetto delle disposizioni ivi contenute.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate,

- il Datore di Lavoro è tenuto all'informativa periodica, almeno su base semestrale, all'Organismo di Vigilanza e al RPCT, riepilogativa degli aggiornamenti relativi ai rischi evidenziati ed alle misure di controllo stabilite ed alle responsabilità ed ai poteri attribuiti in materia di sicurezza sul lavoro;
- il Responsabile del sistema di gestione della sicurezza è tenuto all'informativa periodica all'Organismo di Vigilanza e al RPCT, almeno su base semestrale, in merito allo stato di conformità legislativa;
- il Referente per la sicurezza sui cantieri è tenuto all'informativa periodica all'Organismo di Vigilanza e al RPCT, almeno su base semestrale, in merito alle attività di monitoraggio circa l'operato del CSP/CSE.

III.3.2.3. Attuazione e funzionamento

Il **Datore di lavoro e/o suo delegato**, anche per il tramite dei referenti nominati ed in collaborazione con il Responsabile del sistema di gestione, il RSPP, il MC e le funzioni interne competenti, **assicura**, nel rispetto della normativa vigente:

- **l'informazione, la formazione e l'addestramento del personale aziendale,** a tutti i livelli e in relazione alla mansione svolta, anche attraverso la verifica di apprendimento e di efficacia del modello formativo

adottato;

- **la partecipazione e consultazione dei lavoratori,** anche nell'ambito delle riunioni periodiche previste dalla normativa vigente e per il tramite del loro Rappresentante, nelle diverse attività del sistema di gestione;
- **la programmazione e gestione delle visite mediche** e, più in generale, della sorveglianza sanitaria;
- **in relazione ai fornitori, appaltatori e contraenti, in caso di lavori, servizi e forniture** ha l'obbligo di verificare attraverso l'elaborazione del DUVRI l'idoneità tecnico professionale, della congruità dei costi non soggetti a ribasso relativi alla sicurezza, la valutazione dei rischi da interferenza, nonché la presenza nei contratti di appalto/fornitura di specifiche clausole di risoluzione e sanzionatorie in caso di violazione/omissione del rispetto dei requisiti normativi a loro applicabili o imposti dalla Società;
- **l'adeguatezza e l'integrità degli asset aziendali** attraverso periodiche verifiche manutentive e di conformità ad opera di personale qualificato e idoneo;
- **la gestione tempestiva degli incidenti e delle emergenze** attraverso la predisposizione e la verifica di efficacia di opportuni piani di emergenza e di gestione del rischio incendio;
- **la salute e sicurezza dei lavoratori in trasferta** presso cantieri, fornitori o partner, attraverso: il trasferimento al trasfertista di tutte le informazioni/formazione necessarie allo svolgimento in sicurezza delle attività presso la sede di destinazione; la verifica, da parte del MC, dell'idoneità del trasfertista a svolgere le attività nella sede di destinazione e che lo stesso sia in possesso dei DPI necessari allo svolgimento in sicurezza delle attività; la garanzia che in loco, se non fatto in via preventiva dalla sede, vengano fornite tutte le informazioni necessarie e relative alla gestione delle emergenze, vie di fuga, allarmi, etc. nonché sull'utilizzo dei DPI per l'accesso a specifiche aree; la formalizzazione delle modalità operative per l'autorizzazione allo svolgimento delle attività in trasferta. Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate, il Responsabile del sistema di gestione è tenuto all'informativa periodica, almeno su base annuale, all'Organismo di Vigilanza, riepilogativa della formazione svolta, delle riunioni periodiche e delle prove di emergenza effettuate.
- La popolazione dei lavoratori di Infratel viene differenziata per classi di rischio, ed in particolare sono evidenziati specifici protocolli per il rischio di cantiere. La società si dota di procedure a tutela dalle aggressioni sul luogo di lavoro da parte di soggetti esterni o lavoratori.

Il RSGSSL comunica annualmente all'OdV il documento "Analisi dei rischi-opportunità" ed il conseguente piano degli interventi di adeguamento e di azioni di miglioramento; inoltre, in funzione della gravità dell'evento accaduto, valuta se effettuare una comunicazione tempestiva.

III.3.2.4. Verifica e azioni correttive

Il **Datore di lavoro e/o suo delegato assicura**, nel rispetto della normativa vigente, anche per il tramite dei Referenti nominati ed in collaborazione con il Responsabile del sistema di gestione, il RSPP e il MC:

- la costante registrazione, la **misura e il monitoraggio periodico delle performance degli elementi del sistema sicurezza**, tra cui il grado di conseguimento degli obiettivi di miglioramento, l'efficacia dei controlli definiti, i dati riguardanti le malattie professionali, gli incidenti e la sicurezza degli impianti;
- **l'analisi degli infortuni/incidenti e delle malattie professionali** al fine di identificarne le possibili cause, quindi definire le opportune azioni correttive, preventive e di miglioramento continuo;
- la **gestione delle criticità del sistema**, attraverso la loro identificazione, l'analisi delle cause e la definizione delle opportune azioni correttive/preventive;
- la **conduzione di periodiche verifiche ispettive interne**, da parte dell'Internal Auditing della Capogruppo ovvero di soggetti qualificati ed indipendenti, oggetto di reporting verso il vertice aziendale (Datore di lavoro e Consiglio di Amministrazione) finalizzate a determinare se il sistema di gestione sia conforme ai requisiti stabiliti, sia correttamente attuato e mantenuto attivo.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate, il Responsabile del sistema di gestione è tenuto all'informativa periodica, su base semestrale, all'Organismo di Vigilanza e, se di competenza, al RPCT, riepilogativa degli incidenti occorsi, delle non conformità rilevate, degli esiti delle attività di monitoraggio e di verifica ispettiva. inoltre, in funzione della gravità dell'evento accaduto, valuta se effettuare una comunicazione tempestiva.

L'Ufficio Qualità, Privacy e Sicurezza comunica tempestivamente all'Organismo di Vigilanza, al RPCT, se di competenza, e all'Amministratore Delegato le eventuali azioni correttive conseguenti agli esiti dei controlli a campione sulla correttezza dell'operato delle funzioni assegnatarie.

III.3.2.5. Riesame della Direzione

Il **Datore di lavoro** e/o suo delegato assicura, anche per il tramite del Rappresentante della direzione ed in collaborazione con il Responsabile del sistema di gestione:

- la conduzione su base annuale di almeno **una riunione di riesame del sistema di gestione della sicurezza**, finalizzata a valutarne l'adeguatezza, l'efficacia e le possibilità di miglioramento;
- la **comunicazione dei risultati del riesame al vertice** aziendale (Datore di lavoro e Consiglio di Amministrazione) ed ai soggetti interessati.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate, il Delegato del datore di lavoro è tenuto a comunicare tempestivamente all'Organismo di Vigilanza e al RPCT il Verbale del riesame.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate all'OdV e al RPCT, l'Ufficio Qualità, Privacy e Sicurezza è tenuta alla comunicazione periodica, su base semestrale, all'OdV, al RPCT e alla funzione Acquisti, Affari Generali e Demand Organizzazione di un'informativa riepilogativa relativa a rimozioni, usura, danneggiamenti e dismissione delle dotazioni di sicurezza aziendali, anche indicativa dell'inventariazione degli asset e dei soggetti assegnatari, con l'indicazione di eventuali criticità aperte. inoltre, in funzione della gravità dell'evento accaduto, valuta se effettuare una comunicazione tempestiva.

Fermo restando l'obbligo di verificare l'adeguatezza della programmazione della formazione e di comunicare tempestivamente le opportune azioni correttive, il RSGSSL comunica annualmente all'OdV il programma e il calendario delle attività formative in materia SSL.

III.3.2.6. Gestione degli aspetti Ambientali

Infratel Italia assicura il rispetto della normativa applicabile in materia ambientale**.**

Il Rappresentante Legale e/o i soggetti da questi delegati/incaricati per la gestione degli aspetti ambientali della Società, in collaborazione con l'Ufficio Acquisti, Servizi Generali e la Funzione Legale per gli aspetti di pertinenza, sovraintendono e garantiscono la verifica e il monitoraggio della modalità di gestione dei rifiuti da parte dei fornitori, appaltatori o manutentori:

- le modalità di caratterizzazione dei rifiuti prodotti;
- le modalità di attuazione del Sistema di tracciabilità dei rifiuti, laddove operativo e applicabile, anche in relazione alla tipologia di accordo contrattuale con le ditte di trasporto e smaltimento;
- la compilazione e gestione della documentazione obbligatoria di legge, registri di carico/scarico e formulari di identificazione del rifiuto;

- la corretta gestione del deposito temporaneo dei rifiuti;
- la verifica di rispondenza degli estremi delle autorizzazioni di riferimento per i rifiuti conferiti e della quarta copia del formulario nei termini previsti dalla legislazione vigente.

Nella gestione dei fornitori per la realizzazione e la manutenzione delle infrastrutture di rete, i relativi contratti/accordi quadro dovranno prevedere:

- **clausole di responsabilità in capo all'appaltatore** quale produttore dei rifiuti prodotti/derivanti dall'esecuzione delle attività in cantiere;
- **l'obbligo, in capo all'appaltatore,** di poter operare solo se ottenute tutte le necessarie **autorizzazioni ambientali** (anche per impianti e macchinari) e di avvalersi di ditte debitamente autorizzate per il trasporto e lo smaltimento dei rifiuti;
- **l'obbligo in capo all'appaltatore** di fornire su richiesta ad Infratel Italia la documentazione attestante il possesso dei requisiti abilitativi degli operatori incaricati dallo stesso per il trasporto e lo smaltimento dei rifiuti;
- **l'obbligo, in capo all'appaltatore**, **di comunicazione agli enti di controllo**, secondo le modalità indicate all'art. 242 del Testo Unico Ambientale, nonché di informativa tempestiva all'Amministratore Delegato e/o al suo Delegato/incaricato in materia ambientale, in caso di potenziale inquinamento delle matrici ambientali e la totale responsabilità dell'appaltatore in caso di cagionato inquinamento delle stesse;
- **clausole di disponibilità dell'appaltatore ad essere sottoposto ad** audit di seconda parte effettuati da o per conto di Infratel Italia;
- **penali e/o clausole di risoluzione dei contratti per inadempienze sulla gestione ambientale** ovvero per mancato rispetto degli obblighi normativi ex D.Lgs. 152/2006.

Infratel Italia verifica il possesso dei requisiti abilitativi da parte degli operatori incaricati dall'appaltatore che realizza l'infrastruttura delle attività di trasporto e smaltimento dei rifiuti (presenza autorizzazione e certificazioni in corso di validità, impianti e mezzi di trasporto)

Il Rappresentante legale e/o i soggetti da questi delegati/incaricati per la gestione degli aspetti ambientali, coadiuvati dal Responsabile del sistema di gestione della sicurezza e dai soggetti indicati nel Piano Emergenze ed Evacuazione relativo ai siti aziendali, sovraintendono e garantiscono la **definizione e la corretta attuazione di opportune misure di prevenzione e gestione incendi**, in accordo a quanto stabilito dal Modello 231, Parte Generale e Parte Speciale in materia di sicurezza sul lavoro e dalle procedure del sistema di gestione di Infratel Italia.

Il Rappresentante legale e/o i soggetti da questi delegati/incaricati per la gestione degli aspetti ambientali, anche in collaborazione con le funzioni competenti, **assicurano, al verificarsi di un evento potenzialmente in grado di contaminare un sito di responsabilità di Infratel Italia**, anche avvalendosi di fornitori esterni qualificati e come sopra selezionati, la messa in atto delle procedure di comunicazione agli enti competenti, di **prevenzione della diffusione della contaminazione ed eventualmente di bonifica del sito, conformemente ai disposti di cui all'art. 242 del Testo Unico Ambientale**.

Qualora il sito venga dichiarato inquinato, la Società assicura:

- **l'identificazione di elementi di potenziale contaminazione** (attuale o storica) ai fini della valutazione di avviamento delle necessarie attività di messa in sicurezza e di bonifica;
- **la presentazione del progetto operativo di bonifica o di messa in sicurezza operativa o permanente** (e, ove necessario, le ulteriori misure di riparazione e di ripristino ambientale) entro i termini previsti dall'approvazione del documento di analisi di rischio;

- approvato il progetto, con o senza prescrizioni**, l'attuazione degli interventi di bonifica, messa in sicurezza permanente e messa in sicurezza operativa**, conformemente al progetto approvato;
- la predisposizione della **documentazione da presentare alle autorità competenti** al completamento dell'intervento, **ai fini del rilascio della certificazione di avvenuta bonifica**;
- il **monitoraggio delle procedure operative ed amministrative** nel rispetto delle modalità e delle tempistiche previste dalla normativa vigente.

A tutti i destinatari del Modello 231 - Parte Speciale è fatto inoltre obbligo di osservare tutti i dettami previsti da leggi e regolamenti in materia ambientale (oggi riconducibili al D.Lgs. 152/2006 – Testo Unico Ambientale e s.m.i.).

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate, l'A.D. e/o i soggetti da questi delegati/incaricati per la gestione degli aspetti ambientali della Società e/o il responsabile del sistema di gestione integrato qualità e ambiente comunicano tempestivamente all'OdV e al RPCT le anomalie e/o criticità riscontrate rispetto ai dettami previsti da leggi e regolamenti in materia ambientale. In ogni caso, il responsabile del sistema di gestione integrato qualità e ambiente comunica all'OdV e al RPCT, con cadenza almeno annuale, le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

Il Responsabile dell'Ufficio Qualità, Privacy e Sicurezza è responsabile, oltre all'Amministratore Delegato e agli altri Soggetti titolati di Infratel Italia, del rispetto dei suddetti elementi di controllo.
L'unità QPS cura, inoltre, l'attività di assistenza nei confronti dell'Autorità a norma dell'art.96 del Codice delle comunicazioni elettroniche, garantendo la corrispondenza tra i dati comunicati all'AG e quelli ricevuti dalle funzioni coinvolte.
L'Ufficio Qualità, Privacy e Sicurezza comunica tempestivamente all'Organismo di Vigilanza, al RPCT e all'Amministratore Delegato le notizie di illecito ai sensi dell'art. 174-sexies L. 633/1941.

Per i flussi di dettaglio fare riferimento all'allegato "Flussi OdV e RPCT" del Modello di organizzazione, gestione e controllo ex D.lgs n. 231/01 sezione Qualità, Privacy e Sicurezza.

III.3.2.7. Ulteriori attività di supporto gestionale e di controllo affidate alla funzione Qualità, Privacy e Sicurezza

Tra le responsabilità dell'unità organizzativa Qualità, Privacy e Sicurezza vi sono quelle del Data Protection Officer, rispetto al quale il responsabile svolge un'attività di vigilanza e consulenza circa l'adeguamento della Società alla normativa, anche eurounitaria, di riferimento, e l'adempimento di tutti gli obblighi prescritti in materia di trattamento dei dati personali. Egli, inoltre, nomina e revoca responsabili e/o incaricati del trattamento ai sensi dell'art. 28 G.D.P.R.
Nella mappatura dei rischi tali attività risultano meramente strumentali, in quanto consistono in attività di supporto, coordinamento e monitoraggio prive di un significativo margine di esposizione,funzionali al livello di controllo. Tuttavia, non si può escludere che una grave carenza nel loro svolgimento possa agevolare od occultare la commissione di un illecito, né, altresì, può escludersi che i responsabili di tali funzioni partecipino in concorso con le funzioni coinvolte in altre ipotesi di rischio, divenendo in tal caso essi stessi direttamente autori dell'illecito.
Di seguito il riepilogo delle attività meramente strumentali:

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Presidio delle attività di competenza del Data Protection Officer	DPO ex art. 37 GDPR, PSSLQ	Accesso abusivo a sistema informatico o telematico; danneggiamento di dati o programmi informatici, anche di interesse pubblico; danneggiamento di sistemi informatici o telematici, anche di interesse pubblico;	**RISCHIO STRUMENTALE: Art. 24-bis d.lgs 231/2001 (artt. 615-ter, 635-bis, 635-ter, 635-quater c.p.)**

Al fine di prevenire gli ulteriori rischi di illecito correlati a queste attività meramente strumentali, il *risk owner* di primo livello svolge le proprie attività in coordinamento con le altre funzioni interne e della Capogruppo coinvolte, rispettando i principi generali di controllo e il codice etico, avendo come punti di attenzione i rischi strumentali sopra indicati.
Il process owner garantisce l'effettività e l'efficacia dei controlli, adeguando periodicamente le procedure. A tal fine richiede una informativa ai risk owner, sulla base della quale egli acquisisce le informazioni rilevanti per attuare le opportune azioni correttive e alimentare i flussi informativi, segnalando tempestivamente all'OdV, e al RPCT se di competenza, eventuali anomalie o non conformità riscontrate.

III.3.2.8. Elementi di integrazione tra la gestione dei sistemi informativi e il trattamento dei dati personali.

La Società si conforma alle policies di Capogruppo relative alla gestione dei dati personali e alla gestione dei sistemi informativi (funzione affidata in Service alla Capogruppo), alla cui sezione si fa rimando per quanto qui non riportato. Inoltre, la Società adotta le seguenti misure specifiche: gli account di accesso al sistema informatico da parte degli utenti devono essere univoci e personali, allo scopo di garantire il principio di segregazione dei ruoli; le chiavi d'accesso devono essere aggiornate periodicamente per tutelare la sicurezza informatica del sistema ed impedire frodi sui dati ed accessi abusivi, anche da parte di soggetti interni all'organizzazione stessa; gli accessi sono riportati in file di log ai fini della tracciabilità; sono definiti livelli di accesso differenziato alla intranet aziendale, distinguendo i ruoli secondo le diverse responsabilità; è previsto il monitoraggio dei dati di accesso mediante controlli automatici tramite software o mediante verifiche a campione, adottando cautele per il rispetto della privacy dei lavoratori (pseudonimizzazione dei dati, definizione dei termini di conservazione). In osservanza della disciplina sulla privacy, la competente funzione redige un regolamento sull'uso dei dispositivi informatici ed una procedura per i c.d. "Data Breach", il DPO valuta e monitora l'adeguatezza delle misure adottate e l'impatto di esse sulla privacy. La funzione delegata presidia altresì la documentazione delle modalità di trattamento e la corretta designazione e individuazione dei soggetti del trattamento, comunicando tempestivamente per iscritto le informazioni agli interessati (titolari, responsabili ex art. 28 GDPR, incaricati).

3.3.3.1 Attività a rischio e potenziali reati (Verifiche Cantieri)

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001

Controllo della qualità dei lavori appaltati	Responsabile di funzione/Resp. Qualità, Privacy, Sicurezza, Verificatori.	Falsità in documento pubblico informatico; accesso abusivo a sistema informatico; danneggiamento di dati o programmi informatici, anche di interesse pubblico; danneggiamento di sistemi informatici o telematici, anche di interesse pubblico; concussione; corruzione attiva o passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; ricettazione; riciclaggio; reimpiego in attività produttive o autoriciclaggio di beni di provenienza illecita; malversazione di beni pubblici; truffe, anche informatiche, ai danni di PA centrali o locali; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione attiva o passiva, induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione e istigazione alla corruzione tra privati; omicidio o lesioni gravi e gravissime aggravati dalla violazione delle norme sulla prevenzione degli infortuni sul lavoro e delle malattie professionali; inquinamento ambientale; disastro ambientale; inquinamento e disastro ambientale colposi; uccisione di specie animali o vegetali protette; distruzione di un habitat all'interno di un sito protetto; scarichi di rifiuti; gestione non autorizzata di rifiuti; furto di beni culturali; appropriazione indebita di beni culturali; ricettazione di beni culturali; falsificazione in scrittura privata relativa a beni culturali; vendita non autorizzata di beni culturali/omessa denuncia di cessione; importazione ed esportazione illecita di beni culturali; distruzione di beni culturali; contraffazione di beni culturali; riciclaggio di beni culturali; devastazione o saccheggio di beni culturali	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-ter, 635-quinquies, c.p.);** **Art. 25 d.lgs 231/2001 (artt. 317, 318, 319, 319-quater, 320, 321, 322, c.p.);** **Art. 25-octies d.lgs 231/2001** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 640, 640-bis, 640-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 318, 319, 319-quater, 320, 321, 322, 346-bis);** **Art. 25 ter d.lgs 231/2001 (artt. 2635, 2635-bis c.c.);** **Art. 25-septies d.lgs 231/2001;** **Art. 25-undecies d.lgs 231/2001 (artt. 452-bis, 452-quater, 452-quinquies, 727-bis, 733-bis c.p.; artt. 256, 257 d.lgs n. 152/2006);** **Art. 25 septiesdecies d.lgs 231/2001 (ad eccezione art. 518-quaterdecies);** **Art. 25 duodevicies d.lgs. 231/2001**
Controllo conformità SSL su lavorazioni e materiali di cantiere	Responsabile di funzione	Omicidio o lesioni gravi e gravissime aggravati dalla violazione delle norme sulla prevenzione degli infortuni sul lavoro e delle malattie professionali	**RISCHIO DIRETTO:** **Art. 25-septies d.lgs 231/2001**

3.3.3.2 Elementi di controllo

Infratel, attraverso l'Ufficio Verifiche Cantieri, assicura trasparenza, correttezza e coerenza nelle procedure di verifica della qualità dei lavori eseguiti e nelle attività di collaudo delle opere realizzate, garantendo inoltre la conformità dei cantieri alle disposizioni normative ed aziendali in materia di salute e sicurezza sui luoghi di lavoro.

L'ufficio verifiche Cantieri, quanto al Controllo della qualità dei lavori appaltati e alla Conformità del processo di collaudo, si attiene agli elementi di controllo indicati per l'area Infrastrutture e Operations, cui competono i relativi lavori.

L'attività di controllo di conformità SSL concerne le lavorazioni ed i materiali di cantiere, secondo gli elementi di controllo indicati per la Gestione SSL e indicate in apposita procedura organizzativa per l'area Verifica Cantieri.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate all'OdV, l'Ufficio Verifiche Cantieri è tenuto alla comunicazione periodica, su base semestrale, di un'informativa riepilogativa delle visite di controllo qualità in corso d'opera e dei collaudi effettuati, contenente gli esiti dei controlli e l'indicazione di eventuali non conformità rilevate, attestando, in caso negativo, l'assenza di eventi critici.

III.4 PIANIFICAZIONE, GARE E INGEGNERIA

III.4.1. ATTIVITÀ A RISCHIO E POTENZIALI REATI (PIANIFICAZIONE, GARE E INGEGNERIA)

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Funzioni di RUP	Responsabile di funzione/Responsabile di commessa	Falsità in documento pubblico informatico; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione attiva o passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione e istigazione alla corruzione tra privati; omicidio o lesioni gravi e gravissime aggravati dalla violazione delle norme sulla prevenzione degli infortuni sul lavoro e delle malattie professionali; riciclaggio o rempiego in attività produttive di beni di provenineza illecita; rifiuto d'atti d'ufficio. omissione malversazione di beni pubblici; frode nelle pubbliche forniture; truffe, anche informatiche, ai danni di PA centrali o locali; inquinamento ambientale; disastro ambientale; delitti colposi contro l'ambiente; distruzione o deterioramento di habitat all'interno di un sito protetto; impiego di cittadini di paesi terzi irregolari; favoreggiamento della permanenza illegale dello straniero; dichiarazione ai fini delle imposte dirette o dell'IVA fraudolenta per uso di fatture false oggettivamente o soggettivamente, per altri artifici o altrimenti infedele; occultamento o distruzione dei documenti contabili; compensazione indebita ai danni dell'UE; sottrazione fraudolenta al pagamento di imposte; falsificazione in scrittura privata relativa a beni culturali; esportazione illecita di beni culturali; distruzione di beni culturali; riciclaggio di beni culturali	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (art. 491-bis c.p.);** **Art. 25 d.lgs. 231/2001 (artt. 314, 314-bis, 316, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25 ter d.lgs 231/2001 (art. 2635, 2635-bis c.c.);** **Art. 25-septies d.lgs 231/2001;** **Art. 25-octies d.lgs. 231/2001 (artt. 648-bis, 648-ter c.p.)** **L. 190/2012 (art. 328 c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 356, 640, 640-bis, 640-ter, c.p.);** **Art. 25-ter d.lgs 231/2001 (art. 2635, 2635-bis c.c.);** **Art. 25-undecies d.lgs 231/2001 (art. 452 bis, 452 quater, 452 quinquies, 733-bis c.p.);** **Art. 25-duodecies d.lgs 231/2001;** **Art. 25-quinquiesdecies d.lgs. 231/2001 (art. 2,3, 4, 5, 10, 10-quater, 11 d.lgs. 74/2000);** **Art. 25-septiesdecies d.lgs. 231/2001 (artt. 518-octies, 518-undecies; 518-duodecies c.p.);** **Art. 25-duodevicies d.lgs. 231/2001 (art. 518-sexies, c.p.)**

III.4.2. ATTIVITÀ A RISCHIO E POTENZIALI REATI (GARE E ASSISTENZA RUP)

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Esecuzione, verifiche e adempimenti pre-post procedure di gara	Responsabile di funzione	Turbata libertà degli incanti; turbata libertà del procedimento di scelta del contraente; truffe, anche informatiche, ai danni di PA centrali o locali; falsità in documento pubblico informatico; danneggiamento di dati o programmi informatici, anche di interesse pubblico; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione attiva o passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione e istigazione alla corruzione tra privati; rifiuto d'atti d'ufficio. omissione omicidio o lesioni gravi e gravissime aggravati dalla violazione delle norme sulla prevenzione degli infortuni sul lavoro e delle malattie professionali; ricettazione; riciclaggio; reimpiego in attività produttive o autoriciclaggio di beni di provenienza illecita	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (artt. 353, 353-bis, 640, 640-bis, 640-ter c.p.);** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 635-bis, 635-ter, c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 317, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25-ter d.lgs. 231/2001 (artt. 2635, 2635-bis c.c.)** **L. 190/2012 (art. 328 c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs. 231/2001 (artt. 640, 640-bis, 640-ter c.p.)** **Art. 25-septies d.lgs. 231/2001; Art. 25-octies d.lgs. 231/2001**

Verifiche e monitoraggio subappalto	Responsabile di funzione	Truffe, anche informatiche, ai danni di PA centrali o locali; falsità in documento pubblico informatico; danneggiamento di dati o programmi informatici, anche di interesse pubblico; concussione; corruzione attiva o passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione e istigazione alla corruzione tra privati; malversazione di beni pubblici; omicidio o lesioni gravi e gravissime aggravati dalla violazione delle norme sulla prevenzione degli infortuni sul lavoro e delle malattie professionali; ricettazione; riciclaggio; reimpiego in attività produttive o autoriciclaggio di beni di provenienza illecita; inquinamento ambientale; disastro ambientale; delitti colposi contro l'ambiente; distruzione o deterioramento di habitat all´interno di un sito protetto; impiego di cittadini di paesi terzi irregolari; favoreggiamento della permanenza illegale dello straniero; dichiarazione ai fini delle imposte dirette o dell'IVA fraudolente per l'uso di fatture oggettivamente o soggettivamente false, per altri artifi o altrimenti infedeli; indebita compensazione ai danni dell'UE; falsificazione in scrittura privata relativa a beni culturali; uscita o esportazione illecite di beni culturali; distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici; riciclaggio di beni culturali	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (art. 640, 640-bis, 640-ter c.p.);** **Art. 24-bis d.lgs 231/2001 (art. 491-bis, 635-bis, 635-ter, c.p.)** **Art. 25 d.lgs 231/2001 (artt. 317, 318, 319, 319 quater, 320, 321, 322, 346-bis, c.p.);** **Art. 25-ter d.lgs 231/2001 (art. 2635, 2635-bis c.c.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs. 231/2001 (artt. 316-bis, 640, 640-bis, 640-ter c.p.);** **Art. 25-septies d.lgs 231/2001;** **Art. 25-octies d.lgs. 231/2001;** **Art. 25-undecies d.lgs. 231/2001 (art. 452-bis, 452-quater, 452-quinquies, 733-bis c.p.);** **art. 25-duodecies;** **Art. 25-quiquiesdecies (artt. 2, 3, 4, 10, 10-quater d.lgs. 74/2000);** **Art. 25-septiesdecies d.lgs. 231/2001 (artt. 518-octies, 518-undecies; 518-duodecies c.p.);** **Art. 25-duodevicies d.lgs. 231/2001 (art. 518-sexies c.p.)**

III.4.3. ATTIVITÀ A RISCHIO E POTENZIALI REATI (INGEGNERIA DELLE RETI E DEI SISTEMI)

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001

Sviluppo e sperimentazione di nuove tecnologie delle reti e dei sistemi	Responsabile di funzione	Falsità in documento pubblico informatico; accesso abusivo a sistema informatico; detenzione o installazione di dispositivi atti all'accesso abusivo a sistema informatico; intercettazione o interruzione di conversazioni illegali; detenzione o installazione di apparecchiature atte all'intercettazione o interruzione illegale di comunicazioni; danneggiamento di dati o programmi informatici, anche di interesse pubblico; danneggiamento di sistemi informatici o telematici, anche di interesse pubblico; detenzione o installazione di dispositivi atti ad interrompere un sistema telematico; estorsione informatica; messa a disposizione del pubblico di un'opera dell'ingegno protetta o di parte di essa; duplicazione abusiva di programmi per elaboratore; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori; riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati; abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere scientifiche; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa; omessa segnalazione all'Autorità giudiziaria o alla P.G. di condotte penalmente rilevanti ai sensi della L. n. 633/1941, degli artt. 615-ter e 640-ter c.p.; omessa comunicazione all'AGCOM di un punto di contatto diretto; malversazione di beni pubblici; truffe, anche informatiche, ai danni di PA centrali o locali; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione attiva o passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione e istigazione alla corruzione tra privati; ricettazione; riciclaggio; reimpiego in attività produttive o autoriciclaggio di beni di provenienza illecita; dichiarazione a i fini delle imposte dirette o dell'IVA fraudolente per l'uso di fatture oggettivamente o soggettivamente false, per altri artifici o altrimenti infedeli; omessa dichiarazione; emissione di fatture per operazione inesistenti; occultamento o distruzione di scritture contabili; indebita compensazione ai danni dell'UE	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 615-quater, 615-quater.1, 635-ter, 635-quater, 635-quinquies);** **Art. 25-novies (artt. 171, 171-bis, 171-ter, 174-sexies l. n. 633/1941)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 640, 640-bis, 640-ter c.p.);** **Art. 24-bis d.lgs 231/2001 (artt. 615-quater, 635-ter, 635-quater, 635-quinquies c.p.);** **Art. 25 d.lgs. 231/2001 (artt. 314, 314-bis, 316, 318, 319, 319 quater, 320, 321, 322, 346-bis, c.p.);** **Art. 25-ter c.p. (artt. 2635, 2635-bis c.c.);** **Art. 25-octies d.lgs 231/2001;** **Art. 25-quinquiesdecies d.lgs 231/2001 (artt. 2, 3, 8, 10, 10-quater d.lgs. 74/2000)**
Redazione delle specifiche, norme tecniche e dei capitolati di gara relativi ad affidamenti di lavori, servizi e forniture per tutte le aree operative	Responsabile di funzione	Peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione attiva o passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione e istigazione alla corruzione tra privati; malversazione di beni pubblici; truffe, anche informatiche, ai danni di PA centrali o locali; ricettazione; riciclaggio; reimpiego in attività produttive o autoriciclaggio di beni di provenienza illecita; inquinamento ambientale; disastro ambientale; delitti colposi contro l'ambiente; distruzione o deterioramento di habitat all'interno di un sito protetto	**RISCHIO DIRETTO:** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 318, 319, 319 quater, 320, 321, 322, 346-bis, c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis c.c.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 640, 640-bis, 640-ter c.p.);** **Art. 25 d.lgs. 231/2001 (artt. 314, 314-bis, 316, 318, 319, 319 quater, 320, 321, 322, 346-bis, c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis c.c.);** **Art. 25-octies d.lgs 231/2001;** **Art. 25-undecies d.lgs 231/2001 (artt. 452-bis, 452-quater, 452-quinquies, 733-bis c.p.)**

Omologazione di apparati e materiali da impiegare nelle infrastrutture di rete.	Responsabile di funzione	Ricettazione; riciclaggio; reimpiego in attività produttive o autoriciclaggio di beni di provenienza illecita; truffe, anche informatiche, ai danni di PA centrali e locali; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione attiva o passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione e istigazione alla corruzione tra privati; inquinamento ambientale; disastro ambientale; delitti colposi contro l'ambiente; distruzione o deterioramento di habitat all'interno di un sito protetto	**RISCHIO DIRETTO:** **Art. 25-octies d.lgs 231/2001** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 640, 640-bis, 640-ter c.p.);** **Art. 25 d.lgs. 231/2001 (artt. 314, 314-bis, 316, 318, 319, 319 quater, 320, 321, 322, 346-bis, c.p.);** **Art. 25-ter c.p. (artt. 2635, 2635-bis c.c.);** **Art. 25-octies d.lgs 231/2001;** **Art. 25-undecies d.lgs 231/2001 (artt. 452-bis, 452-quater, 452-quinquies, 452-octies, 733-bis c.p.)**
Predisposizione del listino Infratel e dei relativi prezzi aggiornati secondo le disposizioni di legge	Responsabile di funzione	Truffe, anche informatiche, ai danni di PA centrali o locali; detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; danneggiamento di sistemi informatici o telematici; danneggiamento di sistemi informatici o telematici di pubblico interesse; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione attiva o passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione e istigazione alla corruzione tra privati; ricettazione, riciclaggio; reimpiego in attività produttive o autoriciclaggio di beni di provenienza illecita	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (art. 640, 640-bis, 640-ter c.p.)** **RISCHIO STRUMENTALE:** **Art. 24-bis d.lgs 231/2001 (art. 615-quater, 635-ter, 635-quater, 635-quinquies c.p.);** **Art. 25 d.lgs. 231/2001 (artt. 314, 314-bis, 316, 318, 319, 319 quater, 320, 321, 322, 346-bis c.p.);** **Art. 25-ter c.p. (artt. 2635, 2635-bis c.c.);** **Art. 25-octies d.lgs 231/2001**
Supporto ingegneristico per tutte le funzioni aziendali	Responsabile di funzione	Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; danneggiamento di sistemi informatici o telematici; danneggiamento di sistemi informatici o telematici di pubblico interesse; malversazione di beni pubblici; truffe, anche informatiche, ai danni di PA centrali o locali	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (artt. 615-quater, 635-ter, 635-quater, 635-quinquies c.p.).** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 640, 640-bis, 640-ter c.p.)**
Supporto per l'integrazione dei sistemi aziendali al business dell'azienda	Responsabile di funzione	Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; danneggiamento di sistemi informatici o telematici; danneggiamento di sistemi informatici o telematici di pubblico interesse; malversazione di beni pubblici; truffe, anche informatiche, ai danni di PA centrali o locali	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (artt. 615-quater, 635-ter, 635-quater, 635-quinquies c.p.).** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 640, 640-bis, 640-ter c.p.)**

Collaudo software ed applicazioni	Responsabile di funzione	Falsità in documento pubblico informatico; detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; danneggiamento di sistemi informatici o telematici; danneggiamento di sistemi informatici o telematici di pubblico interesse;messa a disposizione del pubblico di un'opera dell'ingegno protetta o di parte di essa; duplicazione abusiva di programmi per elaboratore; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori; riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati; abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere scientifiche; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa; omessa segnalazione all'Autorità giudiziaria o alla P.G. di condotte penalmente rilevanti ai sensi della L. n. 633/1941, degli artt. 615-ter e 640-ter c.p.; omessa comunicazione all'AGCOM di un punto di contatto diretto; truffe, anche informatiche, ai danni di pa centrali o locali; peculato, peculato mediante profitto dell'errore altrui e indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione e istigazione alla corruzione tra privati; ricettazione; riciclaggio; reimpiego in attività produttive o autoriciclaggio di beni di provenienza illecita	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-quater, 635-ter, 635-quater, 635-quinquies c.p.); Art. 25 novies D. Lgs. 231/2001 (artt. 171, 171-bis, 171-ter, 174-sexies l. n. 633/1941)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 640, comma 2, 640-bis, 640-ter c.p.);** **Art. 25 d.lgs. 231/2001 (artt. 314, 314-bis, 316, 318, 319, 319 quater, 320, 321, 322, 346-bis c.p.);** **Art. 25-ter c.p. (art. 2635, 2635-bis c.c.);** **Art. 25-octies d.lgs 231/2001**

III.4.4. ATTIVITÀ A RISCHIO E POTENZIALI REATI (LEGALE E CONTROLLO OPERATIVO PNRR)

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Gestione degli affari legali relativi ai progetti del PNRR	Responsabile di funzione/Responsabile funzione legale capogruppo/legali esterni/A.D.	Truffe, anche informatiche, ai danni di PA centrali o locali; falsità in documento pubblico informatico; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione attiva o passiva; corruzione in atti giudiziari; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; ricettazione; riciclaggio; reimpiego in attività produttive o autoriciclaggio di beni di provenienza illecita a i fini delle imposte dirette o dell'IVA fraudolente per l'uso di fatture oggettivamente o soggettivamente false, per altri artifici o altrimenti infedeli	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (artt. 640, 640-bis, 640-ter cp);** **Art. 24-bis d.lgs 231/2001 (art. 491-bis cp);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 318, 319, 319-ter, 319 quater, 320, 321, 322, 346-bis c.p.)** **RISCHIO STRUMENTALE:** **Art. 25 d.lgs 231/2001 (artt. 318, 319, 319-ter, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25-octies d.lgs 231/2001;** **Art. 25-quinquiesdecies d.lgs. 231/2001 (artt. 2, 3 e 4 d.lgs 74/2000)**
Compliance DTD e Capogruppo	Responsabile di funzione/Responsabile funzione legale capogruppo	Falsità in documento pubblico informatico; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione attiva o passiva; corruzione in atti giudiziari; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; ricettazione; riciclaggio; reimpiego in attività produttive o autoriciclaggio di beni di provenienza illecita	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (art. 491-bis c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 318, 319, 319-ter, 319-quater, 320, 321, 322, 346-bis c.p.)** **RISCHIO STRUMENTALE:** **Art. 25 d.lgs 231/2001 (artt. 318,**

			319, 319-ter, 319-quater, 320, 321, 322, 346-bis c.p.) **Art. 25-octies d.lgs 231/2001**
Supporto AUDIT PNRR	Responsabile di funzione	Truffa aggravata ai danni dello Stato; falsità in documento pubblico informatico; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione attiva o passiva; corruzione in atti giudiziari; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; ricettazione; riciclaggio; reimpiego in attività produttive o autoriciclaggio di beni di provenienza illecita	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (art. 640 c.p.);** **Art. 24-bis d.lgs 231/2001 (art. 491-bis c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 318, 319, 319-ter, 319-quater, 320, 321, 322, 346-bis c.p.)** **RISCHIO STRUMENTALE:** **Art. 25 d.lgs 231/2001 (artt. 318, 319, 319 ter, 319-quater, 320, 321, 322, 322-bis, 346 bis c.p.);** **Art. 25-octies d.lgs 231/2001**

III.4.5. ATTIVITÀ A RISCHIO E POTENZIALI REATI (PIANIFICAZIONE)

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Redazione degli allegati tecnici dei bandi	Responsabile di processo	Peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione attiva o passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione e istigazione alla corruzione tra privati; malversazione di fondi pubblici; percezione indebita di erogazioni pubbliche; turbata libertà degli incanti; turbata libertà del processo di scelta del contraente; frode nelle pubbliche forniture; truffe, anche informatiche, ai danni di PA centrali o locali; inquinamento ambientale, disastro ambientale; delitti colposi contro l'ambiente; distruzione o deterioramento di habitat all'interno di un sito protetto	**RISCHIO DIRETTO:** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis c.c.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001;** **Art. 25 d.lgs 231/2001 (artt. 318, 319, 319 ter, 319-quater, 320, 321, 322, 322-bis, 346 bis c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis c.c.);** **Art. 25-undecies d.lgs 231/2001 (artt. 452-bis, 452-quater, 452-quinquies, 733-bis c.p.)**
Definizione dei piani tecnici allegati alle Convenzioni con gli Enti finanziatori	Responsabile di funzione, Soggetti titolati	Peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione attiva o passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; induzione indebita a dare o promettere utilità, corruzione attiva e passiva, corruzione in atti giudiziari, istigazione alla corruzione - di membri degli organi UE o di funzionari UE; traffico di influenze illecite; corruzione e istigazione alla corruzione tra privati; malversazione di fondi pubblici; percezione indebita di erogazioni pubbliche; turbata libertà degli incanti; turbata libertà del processo di scelta del contraente; frode nelle pubbliche forniture; truffe, anche informatiche, ai danni di PA centrali o locali; inquinamento ambientale; disastro ambientale; delitti colposi contro l'ambiente; distruzione o deterioramento di habitat all'interno di un sito protetto	**RISCHIO DIRETTO:** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 318, 319, 319-quater, 320, 321, 322, 322-bis, 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis c.c.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001;** **art. 25 d.lgs 231/2001;** **Art. 25-ter d.lgs 231/2001 (art. 2635 c.c.)** **Art. 25-undecies d.lgs 231/2001 (artt. 452 bis, 452 quater, 452 quinquies, 452 octies, 733 bis c.p.)**

III.4.6. ELEMENTI DI CONTROLLO

III.4.6.1. Gestione delle gare.

Come per gli acquisti sottosoglia, anche per gli acquisti che prevedono procedure ad evidenza pubblica ai sensi della normativa sui contratti pubblici, Infratel Italia assicura, attraverso l'**utilizzo dell'Albo fornitori interno o della Capogruppo**, trasparenza, oggettività, pari opportunità e tracciabilità nella selezione degli operatori economici con i quali instaura rapporti di fornitura di beni e servizi di cui si avvale nell'esercizio delle proprie attività.

Infratel Italia assicura che l'acquisizione di lavori, servizi e forniture avvenga nel rispetto dei principi di efficacia, efficienza ed economicità dell'azione amministrativa, oltre che dei principi di libera concorrenza, non discriminazione, proporzionalità e parità di trattamento; la Società svolge puntuali **attività di controllo gerarchico delle funzioni competenti** che partecipano al processo di acquisizione di beni e servizi per la Società.

Ciascuna **richiesta di acquisto** di beni, servizi e lavori da soddisfare **mediante il ricorso ad una procedura ad evidenza pubblica**, deve essere motivata e formalizzata dall'Ufficio richiedente, quindi sottoposta ad **approvazione del titolare di budget**. Qualora una richiesta di acquisto non sia presente nel budget degli acquisti o non via siano risorse sufficienti nel budget dell'Ufficio richiedente, la stessa deve essere sottoposta ad **approvazione da parte dei Soggetti titolati di Infratel Italia**. La funzione richiedente deve fornire nella richiesta di acquisto tutte le informazioni relative alla commessa di riferimento/progetto e, ove applicabile, quelle che consentano di individuare le specifiche tecniche di acquisto nonché una nota motivazionale che definisca ragioni e finalità. **L'Ufficio Gare e Assistenza RUP, di concerto con l'Ufficio Affari Legali della Capogruppo, provvede alla verifica di correttezza, completezza e coerenza della richiesta di acquisto con quanto previsto dalla normativa vigente in materia di appalti pubblici. L'Ufficio Affari Legali presso la Capogruppo è tenuto a verificare eventuali frazionamenti artificiosi degli acquisti.**

A tal proposito l'**Ufficio Gare e Assistenza RUP definisce e formalizza la tipologia di procedura di affidamento a cui fare ricorso**, in base al valore e alle caratteristiche peculiari dell'oggetto dell'affidamento, in conformità con la normativa vigente, nonché l'iter e le modalità operative per lo svolgimento della procedura di affidamento prescelta.

L'Ufficio Gare e Assistenza RUP, l'Ufficio Legale e controllo operativo PNRR e l'Ufficio Affari Legali presso la Capogruppo agiscono, ciascuno per gli aspetti di pertinenza, nel rispetto della normativa vigente in materia di contratti pubblici nella selezione e conduzione della procedura di affidamento, **garantendo** che:

- sia data esecuzione alle sole **forniture ritenute congrue** rispetto ai valori di mercato ed alle esigenze della Società;
- non sia data esecuzione ad alcuna fornitura senza che si sia preventivamente proceduto alla sottoscrizione dell'accordo formale tra le parti (contratto o ordine di acquisto).

L'**Ufficio Gare e Assistenza RUP**, in collaborazione con il Legale e con gli Uffici interni di competenza, assicura:

- la **verifica del possesso**, da parte del fornitore scelto e dell'eventuale subappaltatore, **dei requisiti di affidabilità e onorabilità prestabiliti dall'Ufficio Affari Legali presso la Capogruppo in funzione dell'importo e della tipologia di fornitura**, e dei seguenti altri requisiti:

- il **rispetto** di quanto stabilito in materia dal **Codice dei contratti pubblici** e dalle **leggi antimafia** e **anticorruzione**;

- il rispetto delle disposizioni vigenti in materia di **documentazione antimafia** e di rispetto della **tracciabilità dei flussi finanziari**;

- la verifica del **rating di legalità** e l'iscrizione nell'elenco delle imprese aderenti al protocollo di legalità tra Confindustria ed il Ministero dell'Interno;

- la verifica di non appartenenza della sede legale/operativa del soggetto terzo a Stati segnalati come non cooperativi o a regimi fiscali agevolati, secondo le indicazioni di organismi nazionali e/o sopranazionali operanti nell'antiriciclaggio e nella lotta al terrorismo, nonché la verifica di appartenenza alle "white list" pubblicate dall'Agenzia delle Entrate;

- la verifica di appartenenza alle "white list" pubblicate dalle prefetture competenti, ovvero l'elenco degli operatori economici non soggetti a tentativo di infiltrazione mafiosa, nonché la verifica di **non appartenenza di Soci ed Amministratori alle *"black list"*** di riferimento previste dalle disposizioni legislative vigenti[24];
- la sussistenza nel tempo dei suddetti **requisiti degli operatori economici iscritti all'Albo Fornitori della Capogruppo**, da verificare tramite monitoraggio periodico;
- il rispetto delle **norme contributive, fiscali, previdenziali e assicurative a favore dei propri dipendenti e collaboratori, degli obblighi di tracciabilità finanziaria**, nonché **l'assenza di provvedimenti** a carico dell'ente o dei suoi apicali **per reati** della specie di quelli previsti dal **D.Lgs. 231/01, attraverso la presentazione di una dichiarazione sostitutiva**;
- la verifica circa **l'assenza di situazioni di incompatibilità o di conflitto di interessi in capo al fornitore**, anche attraverso l'acquisizione di una **specifica dichiarazione** attestante l'impegno a non creare tali situazioni per tutta la durata della prestazione. Nel caso in cui il fornitore non sia in grado di produrre tale dichiarazione o sia in condizione di incompatibilità o conflitto d'interesse, **i Soggetti titolati della Società hanno facoltà di procedere in accordo al vigente impianto di procure e deleghe**.

Nell'ambito delle procedure connesse ai procedimenti di affidamento a terzi, sia di appalti nell'ambito del campo di applicazione del codice dei contratti pubblici sia di finanziamenti nell'ambito della concessione di contributi pubblici, Infratel Italia assicura il rispetto dei principi di economicità, efficacia, imparzialità, parità di trattamento, trasparenza, concorrenza, nel processo di selezione degli operatori e garantisce la tracciabilità delle operazioni a tal fine poste in essere. **I soggetti incaricati di assumere decisioni nelle diverse fasi del processo in oggetto vengono identificati sulla base di criteri predefiniti quali inerenza, competenza, professionalità ed esperienza. Tali soggetti non possono autorizzare gli atti di gara ed esercitare gli opportuni controlli sulle operazioni stabilite che sono in capo a soggetti diversi da Infratel Italia.**

Gli Uffici competenti assicurano la **documentabilità, tracciabilità e l'archiviazione** di tutta la documentazione oggetto del procedimento di affidamento, mediante il ricorso ad una **piattaforma informatica** che consente la corretta imputazione di ogni singola operazione ai soggetti che ne sono responsabili, la tracciabilità di ogni operazione effettuata dagli utenti abilitati, l'archiviazione e conservazione delle registrazioni. La Società assicura la **pubblicazione sul proprio sito istituzionale** delle informazioni e dei dati relativi a gare/assegnazione di contributi, in linea con quanto previsto dal Codice degli appalti pubblici e dalla normativa sugli obblighi di pubblicazione e trasparenza da parte delle Pubbliche Amministrazioni.

A tal fine, si rinvia alla procedura operative appositamente predisposta da Infratel per la gestione delle Gare Passive.

La Società, laddove opportuno in relazione alla frequenza/numerosità delle attività poste in essere, si dota di **piani di effettiva rotazione degli incarichi e del personale con funzione di responsabilità** (ivi compresi i Responsabili Unici del Progetto) sulla base di criteri quali competenza, trasparenza, imparzialità e continuità dell'azione amministrativa.

III.4.6.2. Svolgimento del ruolo di RUP per tutti i procedimenti di affidamento per il rispetto degli adempimenti normativi e del sistema di e-procurement. Elaborazione, in collaborazione con la Funzione Rendicontazione, dell'informativa necessaria per la verifica dell'avanzamento e dell'operatività rispetto ai Piani operativi di intervento.

Il Responsabile Unico del Progetto (RUP) è nominato dall'Amministratore Delegato all'interno dell'Ufficio Pianificazione, Gare e Ingegneria, previa verifica circa il possesso dei requisiti tecnico professionali, di indipendenza e dell'assenza di conflitto di interessi ai sensi della normativa vigente. Il RUP, anche in collaborazione con gli Uffici interni competenti, **garantisce** l'adempimento degli obblighi di propria competenza richiesti dalla normativa applicabile, tra cui:

- **l'acquisizione di tutta la documentazione tecnica e amministrativa necessaria all'avvio della procedura di affidamento**, in funzione del tipo di gara/assegnazione di finanziamento[20], nonché la verifica della **completezza della documentazione di progetto**;
- la **definizione**, in conformità a quanto definito nell'accordo/convenzione stipulato con il committente e alle linee guida predefinite dagli Uffici competenti, **della procedura di affidamento e di aggiudicazione, dei criteri e degli atti rilevanti della stessa, sottoponendoli all'approvazione del Presidente/Amministratore Delegato, del Consiglio di Amministrazione e, laddove previsto, del Comitato di Indirizzo**;
- l'**adempimento tempestivo**, nei modi e nei termini previsti dalla normativa applicabile ovvero dagli accordi stipulati con il committente, **degli obblighi di pubblicità** ivi previsti[21], previa sottoscrizione degli atti oggetto di pubblicazione da parte dei Soggetti titolati della Società, in base ai poteri conferiti dal sistema di procure e deleghe in essere;
- la **tracciabilità delle comunicazioni ricevute ed inviate** agli interessati circa lo stato e/o l'esito delle procedure di affidamento poste in essere. Le modalità di comunicazioni con terzi devono garantire l'attuazione tempestiva, in accordo alle disposizioni normative applicabili, delle fasi di protocollazione e adempimento delle richieste/comunicazioni pervenute, anche coinvolgendo gli altri Uffici competenti, al fine di fornire pronto riscontro alle medesime. A tale proposito, il RUP, con il supporto dell'Ufficio Affari Legali presso la Capogruppo, definisce l'iter e le modalità operative per la gestione delle richieste di chiarimenti da parte degli operatori economici e **approva**, in coerenza con il sistema dei poteri vigenti, **le note di chiarimento predisposte a seguito delle richieste pervenute**;
- l'**esecuzione**, avvalendosi della collaborazione degli Uffici competenti, delle **operazioni di affidamento** e delle **verifiche** da condursi, ai sensi della normativa applicabile, **sui requisiti dichiarati** dagli operatori economici in sede di gara;
- **in caso di revoca del bando**, l'attuazione **dell'opportuno iter autorizzativo da parte dei Soggetti titolati della Società**, nonché la formalizzazione e la tracciabilità delle motivazioni che sottendono la revoca, **evidenziando l'eventuale presenza di concreti motivi di interesse pubblico**;
- per tutta la durata della procedura di affidamento, la **conservazione della relativa documentazione** e, al termine della procedura, l'**archiviazione**, nonché la **gestione** della corrispondenza con i concorrenti/potenziali beneficiari.

L'Amministratore Delegato assicura la pianificazione e l'attuazione di controlli a campione volti a verificare la correttezza dell'operato del RUP. A partire dai risultati di tali verifiche, l'Amministratore Delegato **definisce**

20 Bando di gara/finanziamento e allegati, disciplinare di gara/finanziamento, capitolato tecnico e specifiche sui lavori, materiali e apparati.

21 In fase di predisposizione della procedura di affidamento e di conclusione della procedura (aggiudicazione).

eventuali opportune azioni correttive oggetto di comunicazione periodica, su base annuale, all'Organismo di Vigilanza.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate all'**OdV** e al **RPCT**, l'**Ufficio Pianificazione, Gare e Ingegneria** è tenuto alla comunicazione periodica, **su base semestrale,** all'**OdV** ed al **RPCT** di un'informativa riepilogativa dello stato di avanzamento di ciascuna commessa/progetto e delle verifiche effettuate.

In ogni caso, il responsabile dell'Ufficio Pianificazione, Gare e Ingegneria comunica all'OdV e al RPCT, con cadenza almeno annuale, le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

III.4.6.3. Definizione dei Piani Tecnici di Rete nelle Regioni oggetto d'intervento e relativa programmazione per l'attuazione, lo sviluppo e l'evoluzione del Piano di Rete

Il bando di gara per la realizzazione delle infrastrutture di rete contiene, nel rispetto degli accordi formali stipulati con il committente nonché di quanto stabilito dal Codice degli contratti pubblici, **i requisiti**[22] delle società da detenere per l'ammissione alle procedure di gara, le tempistiche e le caratteristiche tecnico economiche delle attività oggetto di realizzazione, i criteri di valutazione e selezione delle offerte, le modalità ed i termini di rendicontazione nonché più in generale le condizioni contrattuali oggetto di gara/bando.
Il processo di valutazione e selezione delle offerte, ovvero di verifica circa il possesso da parte delle società partecipanti dei requisiti stabiliti dal bando[23], avviene attraverso la verifica di tutti i documenti tecnico amministrativi richiesti, secondo le modalità e nel rispetto di quanto previsto dal D. Lgs. 50/2016 e dagli accordi/convenzioni stabiliti con il committente[24].
L'Ufficio Gare e Assistenza RUP definisce la modalità di registrazione e conservazione delle offerte ricevute, anche in caso di procedura telematica, ivi incluse le modalità operative per lo svolgimento delle analisi di anomalia/congruità di offerte anormalmente basse; l'iter e le modalità operative per la verifica della documentazione amministrativa e tecnica, nonché dell'eventuale soccorso istruttorio.

La **graduatoria** delle società ammesse viene **definita da una Commissione di Gara**. **Infratel Italia definisce le modalità operative e i criteri da rispettare per la nomina dei commissari, di competenza del Consiglio di Amministrazione, nonché i requisiti di onorabilità e professionalità degli stessi.** In fase di nomina dei membri della Commissione di Gara, **il RUP assicura la verifica di compatibilità dei soggetti nominati**, ovvero che non sussistano conflitti di interesse[25]. Al termine della verifica **il CdA procede con l'assegnazione definitiva**. È data formale **evidenza delle attività svolte** dalla Commissione di Gara, **mediante** la redazione e sottoscrizione di **appositi verbali**. **I commissari non devono aver svolto né possono svolgere alcun'altra funzione o incarico tecnico o amministrativo relativamente al contratto del cui affidamento si tratta. La nomina a RUP di un membro delle commissioni di gara è valutata con riferimento alla singola procedura.**

I rapporti tra Infratel Italia e gli operatori economici o consulenti (legali, fiscali, tributari, etc..) possono essere disciplinati anche mediante accordi quadro, nel rispetto della normativa vigente in materia applicabile alla

[22] Deve essere tenuta traccia delle motivazioni che hanno condotto alla determinazione di specifici requisiti/criteri di ammissibilità, anche in tema di affidabilità/onorabilità di controparte.
[23] Deve essere garantita la tracciabilità dell'iter di valutazione e selezione
[24] Deve essere garantito il controllo di integrità dei plichi delle eventuali offerte cartacee
[25] Tra cui l'assenza di coinvolgimento in altra funzione/incarico tecnico o amministrativo inerente alla gara/finanziamento

Società: l'affidamento del singolo incarico, nell'ambito dell'accordo quadro di riferimento, avviene previa richiesta formale presentata dall'Ufficio interessato, che indichi l'esigenza, i possibili operatori candidati a seguire l'attività, le motivazioni che sottendono il loro suggerimento (tra cui area di competenza, esperienza pregressa, continuità di azione) ed è sottoposta all'autorizzazione dei Soggetti titolati della Società. I Soggetti titolati della Società stabiliscono in via preventiva: i limiti di importo applicabili ai singoli accordi; i criteri attraverso i quali valutare la congruità delle tariffe applicabili a ciascun accordo quadro, tra cui l'aderenza rispetto ai riferimenti di mercato e alle eventuali disposizioni legislative applicabili.

L'accordo quadro, contratto o convenzione stipulato tra Infratel Italia e l'appaltatore è predisposto dal RUP in collaborazione con l'Ufficio Affari Legali della Capogruppo e gli Uffici competenti di Infratel Italia, quindi sottoposto a firma da parte dei Soggetti titolati della Società sulla base dei poteri ad essi conferiti[26]. Esso contiene specifiche clausole di risoluzione in caso di inosservanza o violazione del Codice Etico e delle previsioni del Modello 231, Parte Generale e Parte Speciale, e del Piano di Prevenzione della Corruzione e della Trasparenza **ex L. 190/2012**, nonché di altre previsioni contrattuali relative alla corretta esecuzione dell'affidamento.
Nei contratti aventi ad oggetto lavori o servizi di scavo sono rispettate tutte le cautele necessarie ad impedire il danneggiamento e l'asportazione di beni culturali, nonché per il rispetto della normativa ambientale.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate all'Organismo di Vigilanza, l'Ufficio Pianificazione, Gare e Ingegneria è tenuto alla comunicazione periodica, su base annuale, di un'informativa riepilogativa di tutte le gare indette, specificandone gli oggetti, gli importi, gli aggiudicatari, i nuovi contratti/accordi/convenzioni sottoscritti e una tempestiva comunicazione al RPCT di tutti i singoli nuovi contratti/accordi/convenzioni sottoscritti, al fine di adempiere agli obblighi relativi alla normativa sulla "trasparenza".

In ogni caso, il responsabile dell'Ufficio Pianificazione, Gare e Ingegneria comunica all'OdV e al RPCT, con cadenza almeno annuale, le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

III.4.6.4. Supporto alla Direzione nella definizione dei Piani operativi pluriennali Definizione dei Piani di commessa e relativi Piani tecnici.

Infratel Italia assicura la regolare esecuzione delle attività svolte per conto della committente (attività di Commessa o Progetto), nel rispetto di quanto previsto nel contratto/convenzione e nel Piano associato.
L'Ufficio Gare e Assistenza RUP supporta e collabora con i Responsabili di Commessa/RUP, opportunamente identificati e nominati dall'Amministratore Delegato[27], nelle attività di sviluppo e per il monitoraggio di tempi e costi di ciascuna commessa o progetto.
L'Ufficio in esame è tenuto ad elaborare e a mantenere aggiornato il Piano tecnico al contratto/convenzione, contenente l'indicazione delle aree e dell'oggetto di intervento, del costo complessivo e del cronoprogramma.
Il Responsabile di Commessa/RUP, in collaborazione con l'Ufficio Gare e Assistenza RUP, anche per le opportune verifiche di qualità, è tenuto a monitorare il rispetto del Piano tecnico associato al contratto/convenzione, comunicando eventuali varianti, scostamenti o anomalie all'Ufficio competente delle Business Units, per la definizione di opportune azioni.
Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate, l'Ufficio Pianificazione è tenuto alla comunicazione periodica, su base semestrale, all'Organismo di

26 E' fatto divieto dare esecuzione alle attività senza che si sia preventivamente proceduto alla sottoscrizione dell'accordo formale tra le parti

27 Sulla base di criteri prestabiliti tra cui esperienza, competenza e ottimizzazione logistica

Vigilanza ed al RPCT di un'informativa riepilogativa dello stato di avanzamento di ciascuna commessa/progetto. Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate all'OdV e al RPCT, per quanto di competenza, l'Ufficio Pianificazione, in coordinamento con l'Ufficio Ingegneria delle Reti e dei Sistemi, è tenuto alla comunicazione periodica, su base annuale, di un'informativa riepilogativa degli allegati tecnici dei bandi e dei piani tecnici delle convenzioni.

In ogni caso, il responsabile dell'Ufficio Pianificazione, Gare e Ingegneria comunica all'OdV e al RPCT, con cadenza almeno annuale, le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

III.4.6.5. Processo di Data Integration di tutte le aree operative finalizzato a fornire i dati per il reporting aziendale

La gestione dei sistemi informativi di Infratel Italia è curata dalla Capogruppo e regolamentata nell'ambito di opportuni contratti di *outsourcing* contenenti clausole di salvaguardia con riferimento, in particolare, alla Sicurezza dei Sistemi - nel rispetto delle politiche e degli elementi a presidio del rischio IT[28] stabiliti dal modello di organizzazione, gestione e controllo della Capogruppo ed anche declinati nel presente documento- e al rispetto di specifici *Service Level Agreement*. Quindi per gli elementi di controllo relativi si rinvia al paragrafo relativo all'area Sistemi Informativi nell'ambito delle attività sensibili/strumentali affidate in service alla Capogruppo con riferimento anche al ruolo dei Referenti interni responsabili della gestione di eventuali sistemi, applicativi e *Data Base* proprietari o di terzi (e quindi non di proprietà della Capogruppo).

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate all'OdV, l'Ufficio Ingegneria delle Reti e dei Sistemi è tenuto alla comunicazione periodica, su base semestrale, di un'informativa riepilogativa dei report elaborati, fornendo una descrizione del contenuto e della finalità dei report, dei soggetti richiedenti e destinatari degli stessi.

In ogni caso, il responsabile dell'Ufficio Ingegneria delle reti e dei sistemi comunica all'OdV e al RPCT, con cadenza almeno annuale, le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

III.4.6.6. Gestione dei servizi di ingegneria. Sviluppo e sperimentazione di nuove tecnologie e sistemi.

L'**Ufficio Ingegneria delle Reti e dei Sistemi** ricopre un ruolo centrale ai fini del raggiungimento degli obiettivi di Infratel Italia, svolgendo una continua attività di *scouting* tecnologico al fine di acquisire informazioni costantemente aggiornate sulle ultime innovazioni tecniche e consentire una valutazione in ordine all'opportunità del loro inserimento nelle attività della Società, sia in riferimento ai processi produttivi, ai prodotti o servizi offerti, sia in relazione ai sistemi, software e programmi impiegati. Provvede altresì, secondo principi di trasparenza, completezza e chiarezza, all'archiviazione dei risultati delle relative ricerche e dei materiali reperiti. Si rinvia a quanto definito nel paragrafo "elementi di controllo Gestione dei rapporti con i soggetti privati", del Capitolo II, relativamente ai rapporti trasversali.

Le modalità di archiviazione dati sono riportate in dettaglio nelle procedure.

[28] Anche con riferimento a sistemi/apparecchiature fuori sede ed in relazione ai rischi connessi all'operare al di fuori del perimetro dell'organizzazione

III.4.6.7. Individuazione dei requisiti tecnici e redazione dei capitolati di gara.

L'**Ufficio Ingegneria delle Reti e dei Sistemi** provvede inoltre alla redazione dei capitolati tecnici relativi alla costruzione, consegna e manutenzione delle infrastrutture di rete, nonché alle attività di competenza di tutte le altre Unità organizzate. Queste ultime, inoltre, possono rivolgere all'Ufficio specifiche richieste di indicazione di norme o specifiche tecniche.

Redatto il capitolato tecnico previo coordinamento con la funzione interessata, l'Ufficio lo invia al responsabile di Pianificazione, Gare e Ingegneria per la verifica e l'approvazione.

Le norme tecniche recepiscono le norme degli enti di settore pertinenti all'argomento e le disposizioni di legge in materia e le regole di buona prassi.

III.4.6.8. Omologazione di materiali e apparati.

L'**Ufficio Ingegneria delle Reti e dei Sistemi** è responsabile del processo di omologazione dei materiali e degli apparati utilizzati nella realizzazione della rete. A tal fine, compie specifiche verifiche al fine di accertare la conformità tra le specifiche tecniche richieste e i materiali indicati dalla ditta appaltatrice, cui richiede la documentazione pertinente, a seguito dell'aggiudicazione del bando, comunicando l'esito al RUP. L'Ufficio, inoltre, anche dopo il processo di omologazione, può chiedere di poter effettuare, tramite propri referenti, test e verifiche sul materiale omologato, a tal fine, sono previste specifiche clausole nei capitolati tecnici e nei contratti, che consentono lo svolgimento delle predette verifiche.

III.4.6.9. Predisposizione del listino Infratel.

L'**Ufficio Ingegneria delle Reti e dei Sistemi** predispone ed aggiorna il listino prezzi relativo alle attività svolte da Infratel Italia e provvede al relativo invio al responsabile di Pianificazione, Gare e Ingegneria per la verifica e all'A.D. per l'approvazione. Viene utilizzato come riferimento il prezziario DEI basato sui costi medi nazionali con eventuale confronto/integrazione voci derivate dai prezziari regionali. In caso di tecnologie e attività non censite, valuta la congruità in relazione al costo delle alternative esistenti sul mercato (anche in relazione al rapporto costo/beneficio della realizzazione con tecnologie alternative), che siano comparabili sul piano operativo e quantitativo. La documentazione è tracciata per la conservazione dei dati come da procedura.

III.4.6.10. Integrazione dei dati provenienti dalle altre unità organizzative e predisposizione dei report aziendali.

L'Ufficio Ingegneria delle reti e dei Sistemi analizza la tipologia e la struttura dei dati contenuti nei vari sistemi aziendali, individuando le specifiche tecniche necessarie ad aggregarli al fine di renderli fruibili all'interno degli strumenti informatici adottati dalla Società, nell'ambito delle attività di reporting aziendale.

III.4.6.11. Collaudo di software e applicazioni.

Con riferimento allo sviluppo informatico, l'Ufficio **Ingegneria delle Reti e dei Sistemi** riceve le richieste provenienti da tutte le funzioni aziendali relative all'esigenza di predisposizione di nuovi sistemi informatici o all'elaborazione di software, procedendo a redigere un apposito studio di fattibilità che provvede ad archiviare per la tracciabilità. L'Ufficio inoltre predispone appositi capitolati tecnici relativi ai bandi per lo sviluppo o l'aggiornamento dei sistemi informatici che vengono sottoposti al responsabile di Pianificazione Gare e Ingegneria, per la verifica e all'AD per l'approvazione. Procede inoltre al monitoraggio dell'attività di sviluppo e programmazione nonché alle attività di collaudo in contraddittorio con l'appaltatore. Propone una test-list ed effettua le operazioni redigendo apposito verbale. Il rilascio in ambiente di produzione avviene solo in caso di esito positivo del collaudo. Nel caso di nuova elaborazione di *software* la funzione verifica l'originalità del

prodotto e la liceità dell'uso in relazione alla tutela del diritto d'autore. Si osserva, nel caso siano acquisiti *software* o parti di *software* di proprietà di terzi, la procedura prevista per l'area "Acquisti" in ordine alla verifica della provenienza e della liceità dell'uso per la tutela del diritto d'autore.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate all'Organismo di Vigilanza, l'Ufficio Ingegneria delle Reti e dei Sistemi è tenuto alla comunicazione periodica, su base annuale, di un'informativa riepilogativa dei materiali e apparati omologati, delle modifiche alle voci di listino e delle relative motivazioni, dei software collaudati e dei soggetti richiedenti il collaudo.

In ogni caso, il responsabile dell'Ufficio Ingegneria delle reti e dei sistemi comunica all'OdV e al RPCT, con cadenza almeno annuale, le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

III.4.6.12. Legale e Controllo Operativo PNRR

L'**Ufficio Legale e Controllo Operativo PNRR** si occupa in primo luogo delle attività di controllo in relazione a tutte le unità operative, assicurando il costante rispetto della normativa vigente nei piani in cui Infratel Italia agisce in qualità di soggetto attuatore degli interventi previsti dal PNRR. A tal fine, pianifica le attività di controllo programmando e predisponendo appositi piani di controllo che vengono sottoposti all'AD per la relativa approvazione. L'Ufficio conduce le attività di controllo attraverso la formazione di appositi Gruppi di Lavoro. L'Ufficio comunica il Piano di Controllo ai responsabili delle funzioni interessate, esegue i relativi controlli ed espone i propri rilievi sulle criticità riscontrate ai responsabili delle funzioni interessate nel corso della riunione finale, indicando altresì le azioni correttive ritenute opportune. I risultati dell'attività di controllo sono compendiati in una relazione finale che viene trasmessa dal responsabile dell'Ufficio all'AD e ai responsabili di primo livello delle funzioni interessate.

L'Ufficio Legale e Controllo Operativo PNRR offre inoltre supporto legale al RUP nella fase di esecuzione dei contratti PNRR e in relazione al contenzioso relativo al PNRR. In particolare, riceve le richieste dei RUP relative alla risoluzione di questioni giuridiche inerenti al PNRR, offrendo pareri legali, anche in ordine alla contrattualistica, ovvero attivando professionisti esterni nel rispetto delle *policies* aziendali e della normativa vigente.

L'Ufficio, in relazione al contenzioso attivo o passivo, provvede alla trasmissione, all'Ufficio Affari Legali di Invitalia, della notifica del provvedimento introduttivo del giudizio o la documentazione su cui fonda l'esigenza di esperire apposite azioni giudiziarie, richiedendo la nomina di un legale esterno, fornendo a quest'ultimo le indicazioni per la definizione della strategia processuale e la documentazione necessaria all'espletamento dell'incarico. L'Ufficio inoltre coadiuva il vertice aziendale nella valutazione circa l'opportunità di accettare, o formulare, una proposta transattiva.

La documentazione di pareri, note e contenziosi sono tracciate e conservate nel rispetto dei termini minimi di legge. Per l'attivazione del contenzioso la funzione Legale e controllo operativo si coordina con la funzione Affari Legali della Capogruppo. La documentazione è tracciata come da procedura.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate all'OdV, l'Ufficio Legale e Controllo Operativo PNRR è tenuto alla comunicazione periodica, su base annuale, di un'informativa riepilogativa dei controlli effettuati, dei pareri legali forniti in merito ai contratti attivi e passivi legati al PNRR, nonché delle altre attività di supporto fornite, dei soggetti richiedenti e i destinatari degli stessi.

In ogni caso, il responsabile dell'Ufficio Legale e Controllo operativo PNRR comunica all'OdV e al RPCT, con cadenza almeno annuale, le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

III.4.6.13. Ulteriori attività di supporto gestionale e di controllo affidate alla funzione Pianificazione, Gare e Ingegneria.

Tra le responsabilità dell'unità organizzativa Pianificazione, Gare e Ingegneria vi sono quelle del Supporto Gare sopra soglia ed e-procurement nonché l'Assistenza RUP (processo Gare e assistenza RUP); l'Integrazione dei dati provenienti da tutte le aree operative e la Predisposizione di report relativi ai piani operativi (processo Ingegneria delle Reti e dei Sistemi); la gestione dei Piani di controllo PNRR (processo Legale e Controllo operativo PNRR); infine, il Procedimento di consultazione periodica per la mappatura della copertura del territorio nazionale con reti fisse e mobili, il Monitoraggio e revisione periodica dei piani e l'Elaborazione di scenari e studi di fattibilità per nuovi programmi e opportunità di finanziamento (processo Pianificazione)

Nella mappatura dei rischi tali attività risultano meramente strumentali, in quanto consistono in attività di supporto, coordinamento e monitoraggio prive di significativi elementi di esposizione e tipiche della funzione di controllo o di pianificazione strategica. Tuttavia, non si può escludere che una grave carenza nel loro svolgimento possa agevolare od occultare la commissione di un illecito, né, altresì, può escludersi che i responsabili di tali funzioni partecipino in concorso con le funzioni coinvolte in altre ipotesi di rischio, divenendo in tal caso essi stessi direttamente autori dell'illecito.

Di seguito il riepilogo delle attività meramente strumentali:

AREA	ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
GARE E ASSISTENZA RUP	Supporto Gare sopra soglia ed e-procurement	Responsabile di funzione	Malversazione di beni pubblici; frode nelle pubbliche forniture; truffe, anche informatiche, ai danni di PA centrali o locali; falsità in documento pubblico informatico; accesso abusivo a sistema informatico; danneggiamento di dati o programmi informatici, anche di interesse pubblico; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione attiva o passiva; induzione inebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; omicidio o lesioni gravi e gravissime aggravati dalla violazione delle norme sulla prevenzione degli infortuni sul lavoro e delle malattie professionali; riciclaggio; reimpiego in attività produttive di beni di provenienza illecita; disastro ambientale; delitti colposi contro l'ambiente; distruzione o deterioramento di habitat all´interno di un sito protetto; impiego di cittadini di paesi terzi irregolari; favoreggiamento della permanenza illegale dello straniero; dichiarazione ai fini delle imposte dirette o dell'Iva fraudolente per l'uso di fatture oggettivamente o soggettivamente false, per altri artifici o altrimenti infedeli; omessa dichiarazione; occultamento o distruzione di documenti contabili; indebita compensazione ai danni dell'UE; falsificazione in scrittura privata relativa a beni culturali; uscita o esportazione illecite di beni culturali; distruzione, dispersione,	**RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 356, 640, 640-bis, 640-ter c.p.);** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.);** **Art. 25 d.lgs. 231/2001 (artt. 314, 314-bis, 316, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25-septies d.lgs 231/2001;** **Art. 25-octies d.lgs 231/2001 (648-bis, 648-ter c.p.)** **Art. 25-undecies d.lgs 231/2001 (artt. 452-quater, 452-quinquies, 733-bis c.p.);** **Art. 25 duodecies d.lgs 231/2001;** **Art. 25-quinquiesdecies d.lgs. 231/2001 (art. 2, 3, 4, 5, 10, 10-quater d.lgs. 74/2000);** **Art. 25-septiesdecies d.lgs. 231/2001 (artt. 518-octies, 518-undecies; 518-duodecies c.p.);** **Art. 25-duodevicies d.lgs. 231/2001 (art. 518-sexies, c.p.)**

			deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici; riciclaggio di beni culturali	
	Assistenza RUP	Responsabile di funzione	Malversazione di beni pubblici; truffe, anche informatiche, ai danni di PA centrali o locali; falsità in documento pubblico informatico; accesso abusivo a sistema informatico; danneggiamento di dati o programmi informatici, anche di interesse pubblico; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione attiva o passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione e istigazione alla corruzione tra privati; riciclaggio; reimpiego in attività produttive di beni di provenienza illecita; dichiarazione a i fini delle imposte dirette o dell'IVA fraudolente per l'uso di fatture oggettivamente o soggettivamente false, per altri artifici o altrimenti infedeli; occultamento o distruzione di documenti contabili; indebita compensazione ai danni dell'UE	**RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 640, 640-bis, 640-ter c.p.);** **Art. 24-bis d.lgs 231/2001 (art. 491-bis, 615-ter, 635-bis, 635-ter, c.p.);** **Art. 25 d.lgs. 231/2001 (artt. 314, 314-bis, 316, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis c.c.);** **Art. 25-octies d.lgs 231/2001 (artt. 648-bis, 648-ter c.p.)** **Art. 25-quinquiesdecies d.lgs. 231/2001 (art. 2, 3, 4, 10, 10-quater, d.lgs. 74/2000).**
INGEGNERIA DELLE RETI E DEI SISTEMI	Integrazione dei dati provenienti da tutte le aree operative	Responsabile di funzione	Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; danneggiamento di sistemi informatici o telematici; danneggiamento di sistemi informatici o telematici di pubblico interesse; ostacolo alle funzioni di vigilanza di pubbliche autorità	**RISCHIO STRUMENTALE:** **Art. 24-bis d.lgs 231/2001 (artt. 615-quater, 635-ter, 635-quater, 635-quinquies c.p.);** **Art. 25-ter c.p. (art. 2638 c.c.)**
	Predisposizione di report relativi ai piani operativi	Responsabile di funzione	Malversazione di beni pubblici; truffe, anche informatiche, ai danni di PA centrali o locali; falsità in documento pubblico informatico; detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; danneggiamento di sistemi informatici o telematici; danneggiamento di sistemi informatici o telematici di pubblico interesse; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione attiva o passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione e istigazione alla corruzione tra privati, ostacolo alle funzioni di vigilanza di pubbliche autorità	**RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 640, 640-bis, 640-ter c.p.)** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-quater, 635-ter, 635-quater, 635-quinquies c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art.25-ter c.p. (artt. 2635, 2635-bis, 2638 c.c.)**
LEGALE E CONTROLLO OPERATIVO PNRR	Piani di controllo PNRR	Responsabile di funzione	Corruzione attiva o passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; induzione indebita a dare o promettere utilità, corruzione attiva e passiva, corruzione in atti giudiziari, istigazione alla corruzione - di membri degli organi UE o di funzionari UE; traffico di influenze illecite; ricettazione; riciclaggio; reimpiego in attività produttive o autoriciclaggio di beni di provenienza illecita	**RISCHIO STRUMENTALE:** **Art. 25 D. Lgs. 231/2001 (artt. 318, 319, 319 ter, 320, 321, 322, 322-bis, 346 bis c.p.);** **Art. 25-octies d.lgs 231/2001**
PIANIFICAZIONE	Procedimento di consultazione periodica per la mappatura della copertura del territorio nazionale con reti fisse e mobili	Responsabile di funzione, A.D.	Malversazione di beni pubblici; frode nelle pubbliche forniture; truffe, anche informatiche, ai danni di PA centrali o locali	**RISCHIO STRUMENTALE:** **Art. 24 d.lgs. 231/2001 (artt. 316-bis, 356, 640, 640-bis,**

				640-ter c.p.)
	Monitoraggio e revisione periodica dei piani	Responsabile di funzione, Delegato, A.D., C.D.A.	Malversazione di beni pubblici; frode nelle pubbliche forniture; truffe, anche informatiche, ai danni di PA centrali o locali	**RISCHIO STRUMENTALE: Art. 24 d.lgs. 231/2001 (artt. 316-bis, 356, 640, 640-bis, 640-ter c.p.)**
	Elaborazione scenari e studi di fattibilità per nuovi programmi e opportunità di finanziamento	Responsabile di funzione	Malversazione di beni pubblici; frode nelle pubbliche forniture; truffe, anche informatiche, ai danni di PA centrali o locali	**RISCHIO STRUMENTALE: Art. 24 d.lgs. 231/2001 (artt. 316-bis, 356, 640, 640-bis, 640-ter c.p.)**

Al fine di prevenire gli ulteriori rischi di illecito correlati a queste attività meramente strumentali, il risk owner di primo livello svolge la propria attività in coordinamento con le altre funzioni interne e della Capogruppo coinvolte, rispettando i principi generali di controllo, avendo come punti di attenzione le attività ed i rischi strumentali sopra indicati.
Il process owner garantisce l'effettività e l'efficacia dei controlli, adeguando periodicamente le procedure. A tal fine richiede una informativa ai risk owner, sulla base della quale egli acquisisce le informazioni rilevanti per attuare le opportune azioni correttive e alimentare i flussi informativi, segnalando tempestivamente all'OdV, e al RPCT se di competenza, eventuali anomalie o non conformità riscontrate.

III.5 RAPPORTI CON LA PA, CON GLI ENTI E CON GLI UTENTI

III.5.1. ATTIVITA' A RISCHIO E POTENZIALI REATI (RAPPORTI CON LA PA, CON GLI ENTI E CON GLI UTENTI)

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Gestione mailbox aziendale per relazioni esterne	Segr. Presidenza, Segr. AD, altre segr, IRS, dirigenti, soggetti esterni	Accesso abusivo a sistema informatico; danneggiamento di dati o programmi informatici anche di interesse pubblico; danneggiamento di sistemi informatici o telematici anche di interesse pubblico; falsità in documento pubblico informatico	**RISCHIO DIRETTO: Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter, 635-quater c.p.)**
Aggiornamento siti e altre piattaforme di comunicazione con enti e utenti	Resp. RPAENUT, Service Comunicazione, Amministratore sistema	Accesso abusivo a sistema informatico; danneggiamento di dati o programmi informatici anche di interesse pubblico; danneggiamento di sistemi informatici o telematici anche di interesse pubblico; falsità in documento pubblico informatico; riproduzione illecita di opera altrui; duplicazione illecita di programmi per elaboratore; riproduzione o duplicazione a fini non strettamente personale o detenzione di copie ai fini della cessione; manipolazione del mercato	**RISCHIO DIRETTO: Art. 25-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter, 635-quater c.p.); Art. 25-novies (artt. 171, 171-bis, 171-ter l. 633/1941)** **RISCHIO STRUMENTALE: Art. 25-sexies d.lgs 231/2001 (art. 185 TUF)**
Richiesta e raccolta di report regionali e report mensili relativi all'andamento dei piani, per supporto documentale all'AD negli eventi territoriali	AD, resp. RPAENUT, funzioni coinvolte, soggetti esterni	Accesso abusivo a sistema informatico; danneggiamento di dati o programmi informatici anche di interesse pubblico; danneggiamento di sistemi informatici o telematici anche di interesse pubblico; falsità in documento pubblico informatico; truffe, anche informatiche, ai danni di PA centrali o locali	**RISCHIO DIRETTO: Art. 24-bis d.lgs. 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter, 635-quater c.p.)** **RISCHIO STRUMENTALE: Art. 24 d.lgs. 231/2001 (artt. 640, 640-bis, 640-ter c.p.)**

III.5.2. ELEMENTI DI CONTROLLO PER RAPPORTI CON LA PA, CON GLI ENTI E CON GLI UTENTI

Ai fini della mitigazione del rischio reato nei processi sopra richiamati, si rinvia ai principi generali in tema di

tracciabilità e documentazione, alle misure adottate nei processi “Qualità, Privacy, Sicurezza” e “Gestione dei Sistemi Informativi”, con particolare riferimento alla gestione delle password, della tracciabilità dei dati, della fedeltà delle informazioni riportate e agli elementi di controllo specifici del processo “Acquisti”, per quanto attiene la liceità dell’uso di *software*, immagini e altri beni immateriali soggetti alla disciplina sul diritto d’autore. Si richiamano inoltre gli elementi di controllo per il processo trasversale rapporti con soggetti privati, in ordine alla fedeltà al vero della comunicazione e le regole di comportamento generali in ordine alla gestione delle informazioni riservate.

Fermo restando l’obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate, la funzione Rapporti con la PA, con gli Enti e gli altri utenti è tenuta ad inviare all'OdV, per mezzo dell'Amministratore Delegato di Infratel Italia, un’informativa periodica, su base annuale, riepilogativa degli eventi territoriali effettuati durante l’anno.

In ogni caso, il responsabile dell’Ufficio Rapporti con la PA, con gli Enti e con gli Utenti comunica all’OdV e al RPCT, con cadenza almeno annuale, le non conformità riscontrate, attestando, in caso negativo, l’assenza di eventi critici (positive assurance).

CAPITOLO IV MISURE SPECIFICHE PER GLI ALTRI PROCESSI DI STAFF (IN SERVICE)

IV.1 ATTIVITÀ AFFIDATE ALLA CAPOGRUPPO SULLA BASE DI UN CONTRATTO DI SERVICE

Sulla base di un contratto di service sono affidate alla Capogruppo le seguenti attività:

- Comunicazione
- Affari Legali
- Sistemi Informativi
- Amministrazione e Bilancio
- Risorse Umane e Organizzazione
- Supporto operativo piattaforma di gara

Per tali attività, il responsabile del contratto di service è l'Amministratore delegato di Infratel Italia e i **diversi Soggetti titolati coinvolti sulla base del sistema di procure e deleghe.** Al Presidente è affidata, per la gestione dei soli rapporti istituzionali, la responsabilità del Service Comunicazione. L'unità Acquisiti, Affari Generali e Demand Organizzazione presidia i predetti contratti.

IV.2 COMUNICAZIONE

Sono affidate alla Capogruppo le attività relative alla Gestione dei Siti web non gestiti direttamente da Infratel Italia, alla Rassegna Stampa e al monitoraggio agenzie di stampa, sotto la responsabilità del Presidente del C.d.A. per l'ambito Gestione rapporti istituzionali su Service Comunicazione e in coordinamento con l'unità Rapporti con la PA, con gli Enti e con gli Utenti, per i portali da questa gestiti direttamente.

IV.2.1. ATTIVITÀ A RISCHIO E POTENZIALI REATI (COMUNICAZIONE)

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Gestione degli eventi e delle sponsorizzazioni	Pres./A.D./Resp. funzione Capogruppo/Resp. contratto di service	Malversazione di erogazioni pubbliche; truffa in danno dello Stato o altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; peculato e peculato mediante profitto dell'errore altrui e indebita destinazione di denaro o cose mobili quando i fatti offendono gli interessi finanziari dell'UE; concussione; corruzione attiva o passiva; corruzione in atti giudiziari; induzione indebita a dare o promettere utilità; istigazione alla corruzione; induzione indebita a dare o promettere utilità, corruzione attiva e passiva, corruzione in atti giudiziari, istigazione alla corruzione - di membri degli organi UE o di funzionari UE; traffico di influenze illecite; indebita percezione di erogazioni pubbliche	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 640, 640-bis c.p.);** **Art. 25 d.lgs 231/2001;** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-ter, 640, 640-bis c.p.);** **Art. 25 d.lgs 231/2001**

Gestione degli omaggi, liberalità e spese di rappresentanza	Pres./A.D./Resp. funzione Capogruppo/Resp. contratto di service	Malversazione di erogazioni pubbliche; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; concussione; corruzione attiva o passiva di pubblico ufficiale o incaricato di pubblico servizio; corruzione in atti giudiziari; induzione indebita a dare o promettere utilità; istigazione alla corruzione; induzione indebita a dare o promettere utilità, corruzione attiva e passiva, corruzione in atti giudiziari, istigazione alla corruzione - di membri degli organi UE o di funzionari UE; traffico di influenze illecite; corruzione tra privati; istigazione alla corruzione tra privati; ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.); autoriciclaggio	**RISCHIO DIRETTO:** **Art. 24 d.lgs. 231/2001 (art. 316-bis c.p.);** **Art. 25 d.lgs. 231/2001;** **Art. 25-ter d.lgs. 231/2001 (artt. 2635, 2635-bis c.c.)** **RISCHIO STRUMENTALE:** **Art. 25 octies d.lgs. 231/2001**
Comunicazione web e stampa	Pres. CDA/A.D./ RPAEUT, resp. funzione coinvolta	Manipolazione del mercato; messa a disposizione del pubblico di un'opera dell'ingegno protetta o di parte di essa; duplicazione abusiva di programmi per elaboratore; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori; riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati; abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere scientifiche; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa; omessa segnalazione all'Autorità giudiziaria o alla P.G. di condotte penalmente rilevanti ai sensi della L. n. 633/1941, degli artt. 615-ter e 640-ter c.p.; omessa comunicazione all'AGCOM di un punto di contatto diretto; truffa in danno dello Stato o di altro ente pubblico o dell'UE (art.640, comma 2, n.1, c.p.); truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.); frode informatica in danno dello Stato o di altro ente pubblico o dell'UE	**RISCHIO DIRETTO:** **Art. 25-sexies d.lgs 231/2001 (art. 185 TUF);** **Art. 25-novies d.lgs 231/2001 (artt. 171, 171-bis, 171-ter, 174-sexies L. n. 633/1941)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs. 231/2001 (artt. 640, 640-bis, 640-ter c.p.);** **Art. 25 sexies d.lgs 231/2001 (art. 185 TUF)**

IV.2.2. ELEMENTI DI CONTROLLO COMUNICAZIONE

Per tutte le attività sensibili o strumentali individuate, il Responsabile di processo sensibile e/o strumentale coincide con la Funzione competente di Capogruppo e con il responsabile del contratto di service, ovvero l'Amministratore delegato di Infratel Italia e i diversi Soggetti titolati coinvolti sulla base del sistema di procure e deleghe.

L'Amministratore Delegato e le altre funzioni coinvolte garantiscono la piena conformità delle attività espletate dalla Capogruppo.

IV.2.3. GESTIONE DEGLI EVENTI E DELLE SPONSORIZZAZIONI

Annualmente l'Ufficio Comunicazione presso la Capogruppo elabora, sulla base degli interventi richiesti dalle funzioni aziendali e dal Presidente/Amministratore Delegato di Infratel Italia, un Piano annuale degli eventi e delle sponsorizzazioni, assicurando la coerenza con le strategie di comunicazione previste e definite dal vertice aziendale. Il Piano, comprensivo del budget associato, è approvato dall'Amministratore Delegato di Infratel Italia.

Qualora si verifichino esigenze extra Budget deve essere nuovamente attivato il processo di pianificazione.

La progettazione dei contenuti e delle modalità di sponsorizzazione è operata dall'Ufficio Comunicazione presso

la Capogruppo, in condivisione con l'Amministratore Delegato di Infratel Italia, che è tenuto a formalizzare le motivazioni in base alle quali viene selezionato un ente specifico da sponsorizzare.

Qualora all'evento/sponsorizzazione sia correlato un acquisto, l'Ufficio Comunicazione presso la Capogruppo elabora la richiesta attivando il processo di acquisto di beni/servizi a cui si rimanda per gli elementi di controllo ivi definiti.

Ciascun accordo di sponsorizzazione è formalizzato, previa verifica di affidabilità ed onorabilità di controparte operata - in accordo alle responsabilità ed agli elementi di controllo definiti per il processo di Acquisto - qualora i soggetti terzi non siano enti di natura istituzionale, nell'ambito di un contratto predisposto dall'Ufficio Acquisti, Affari Generali e Demand Organizzazione e debitamente firmato dai Soggetti titolati di Infratel Italia.

La Funzione Comunicazione presso la Capogruppo assicura la gestione del feedback di ciascun evento, documentando i contenuti, l'organizzazione e l'esito.

La Funzione Comunicazione presso la Capogruppo, in collaborazione con l'Ufficio Acquisti interno, verifica la congruità tra il contributo corrisposto/versato per l'evento/sponsorizzazione e la prestazione da ricevere o ricevuta, in relazione ai prezzi di mercato e ai feedback dell'evento/sponsorizzazione.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate, la Funzione Comunicazione presso la Capogruppo, per mezzo dell'Amministratore Delegato di Infratel Italia, è tenuta all'informativa periodica, su base annuale, all'Organismo di Vigilanza ed al RPCT, riepilogativa degli eventi promossi, delle iniziative di sponsorizzazione e promozione effettuate durante l'anno, con l'indicazione per ciascuna di esse della data, dell'importo della promozione/sponsorizzazione e/o delle eventuali spese sostenute, da terze parti coinvolte.

In ogni caso, il responsabile dell'Ufficio Comunicazione presso la Capogruppo comunica all'OdV e al RPCT, con cadenza almeno annuale, le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

IV.2.4. GESTIONE DEGLI OMAGGI, LIBERALITÀ E SPESE DI RAPPRESENTANZA

Infratel Italia assicura che le attività inerenti alla gestione degli omaggi, delle liberalità e delle spese di rappresentanza siano condotte in maniera trasparente e documentabile, nel rispetto delle regole di condotta definite nel Codice Etico.

Gli omaggi devono rientrare nell'ambito del budget di funzione, previsto in fase di pianificazione, e il relativo processo di acquisto deve avvenire nel rispetto dei principi espressi dal Codice Etico e degli elementi di controllo previsti dal processo di acquisto di beni e servizi di Infratel Italia, declinati nel presente documento.

È previsto il divieto di qualsiasi forma di regalo a funzionari pubblici italiani ed esteri, o a loro familiari o intermediari, nonché ai fornitori/partner della Società che possa influenzare la discrezionalità ovvero l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per Infratel Italia.

Le donazioni/liberalità devono rientrare nell'ambito di un budget annuale, predisposto dalle funzioni titolate alla richiesta che ne verbalizzano le motivazioni, approvato dall'Amministratore Delegato.

Le donazioni/liberalità possono essere erogate previo accordo formalizzato con il beneficiario, elaborato dalle funzioni competenti della Società.

Le associazioni/fondazioni in favore delle quali è possibile effettuare donazioni o erogazioni liberali di qualsiasi tipo devono essere enti di rilevanza nazionale o di indubbia affidabilità e onorabilità.

Le spese di rappresentanza sono consentite ai soli Soggetti titolati, autorizzati dall'Amministratore Delegato, nel rispetto di un monte spese da dedicarsi all'attività di rappresentanza definito in fase di elaborazione del budget.

Tutte le spese di rappresentanza devono essere inerenti alle attività aziendali e rendicontate attraverso la predisposizione di una opportuna nota spesa a cui si allegano i relativi giustificativi fiscalmente validi, fornendo l'indicazione della data, della tipologia di spesa, dell'importo e dei soggetti terzi beneficiari.

IV.2.5. COMUNICAZIONE WEB E STAMPA

Infratel Italia assicura nell'ambito della comunicazione esterna il rispetto della normativa applicabile in materia di diritto d'autore. L'informazione deve essere trasparente e veritiera. La pubblicazione di notizie di stampa o sul web non deve essere utilizzata o manipolata per conseguire un indebito vantaggio dell'Ente.
Si rinvia per quanto d'interesse agli elementi di controllo per gestione acquisti, in merito alle verifiche circa la provenienza dei beni coperti da diritto d'autore e agli elementi di controllo per il processo trasversale rapporti con soggetti privati, in ordine alla fedeltà al vero della comunicazione.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate, la funzione Comunicazione presso la Capogruppo è tenuta ad inviare all'OdV, per mezzo dell'Amministratore Delegato di Infratel Italia, un'informativa periodica, su base annuale, riepilogativa degli omaggi, delle liberalità e delle spese di rappresentanza effettuate durante l'anno con l'indicazione per ciascuna di esse del beneficiario, della data, dell'importo e della causale.

In ogni caso, il responsabile dell'Ufficio Comunicazione presso la Capogruppo comunica all'OdV e al RPCT, con cadenza almeno annuale, le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

IV.3 AFFARI LEGALI

Sono affidate alla Capogruppo le attività relative alla **Consulenza legale e alla Segreteria societaria.**
Le attività a rischio (sensibili/strumentali) individuate in tale area sono la gestione dei contenziosi giudiziali e stragiudiziali e la gestione dei rapporti con soggetti coinvolti in procedimenti innanzi all'autorità giudiziaria e le attività del societario/segreteria societaria.

IV.3.1. ATTIVITÀ A RISCHIO E POTENZIALI REATI (AFFARI LEGALI)

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001

Gestione dei contenziosi giudiziali e stragiudiziali	AD, Ufficio interessato, Affari Legali/Legale Societario Controllate (Capogruppo) Legale e Controllo Operativo Risorse Umane (Capogruppo), Referente contratto di servizio	Truffa in danno dello Stato o di altro ente pubblico o dell'UE; falsità in documento pubblico informatico; indebita destinazione di denaro o cose mobili quando il fatto offende gli interessi finanziari dell'UE; concussione; corruzione attiva e passiva; corruzione in atti giudiziari; istigazione alla corruzione; corruzione attiva e passiva, corruzione in atti giudiziari, istigazione alla corruzione - di membri degli organi UE o di funzionari UE; traffico di influenze illecite; ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita; autoriciclaggio; induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria; dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (art. 640 c.p.);** **Art. 24-bis d.lgs 231/2001 (art. 491-bis c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314-bis, 317, 318, 319, 319-ter, 321, 322, 322-bis, 346-bis c.p.)** **RISCHIO STRUMENTALE:** **Art. 25 d.lgs 231/2001 (artt. 318, 319, 319 ter, 321, 322, 346-bis c.p.);** **Art. 25-octies d.lgs 231/2001;** **Art. 25-decies d.lgs 231/2001 (art. 377-bis c.p.);** **Art. 25-quinquiesdecies d.lgs 231/2001 (art. 2 d.lgs 74/2000)**
Gestione dei rapporti con soggetti coinvolti in procedimenti di fronte all'Autorità giudiziaria	Responsabile della funzione cui il soggetto appartiene	Concussione, corruzione in atti giudiziari, istigazione alla corruzione; induzione indebita a dare o promettere utilità, corruzione attiva e passiva, corruzione in atti giudiziari, istigazione alla corruzione - di membri degli organi UE o di funzionari UE; induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità giudiziaria; corruzione attiva e passiva; istigazione alla corruzione; traffico di influenze illecite; ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita; autoriciclaggio; dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti	**RISCHIO DIRETTO:** **Art. 25 d.lgs 231/2001 (artt. 317, 319-ter, 322-bis c.p.);** **Art. 25 decies d.lgs 231/2001 (art. 377-bis c.p.)** **RISCHIO STRUMENTALE:** **Art. 25 d. lgs. 231/2001 (artt. 318, 319, 319 ter, 321, 322, 346-bis c.p.);** **Art. 25-octies d.lgs 231/2001;** **Art. 25-quinquiesdecies d.lgs. 231/2001 (art. 2 d.lgs 74/2000)**

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Segreteria societaria	Responsabile di segreteria	False comunicazioni sociali; False comunicazioni sociali delle società quotate; impedito controllo dei soci o organi sociali; indebita restituzione di conferimenti; illegale ripartizione degli utili e delle riserve; illecite operazioni sulle azioni o quote sociali o della società controllante; operazioni in pregiudizio dei creditori; omessa comunicazione del conflitto d'interessi; formazione fittizia del capitale; indebita ripartizione dei beni sociali da parte dei liquidatori; corruzione tra privati; istigazione alla corruzione tra privati; illecita influenza sull'assemblea; aggiotaggio; Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza	**RISCHIO DIRETTO:** **Art. 25-ter d.lgs 231/2001 (artt. 2621, 2622, 2625, 2626, 2627, 2628, 2629, 2629 bis, 2632, 2633, 2635, 2635 bis, 2636, 2637, 2638 c.c.)**

IV.3.2. ELEMENTI DI CONTROLLO AFFARI LEGALI

L'Amministratore Delegato o altra funzione coinvolta garantiscono la piena conformità delle attività espletate dalla Capogruppo.

IV.3.2.1. Gestione del Contenzioso giudiziale e stragiudiziale

Qualsiasi citazione, ricorso o altro atto introduttivo relativo a contenziosi attivi e passivi, dei quali sia titolare Infratel Italia, deve essere portato a conoscenza immediatamente della Funzione Affari Legali affinché

quest'ultimo concordi con l'Amministratore Delegato le opportune azioni e contromisure.

Qualora una funzione aziendale abbia la necessità di attivare un contenzioso è tenuta a trasmettere alla Funzione Affari Legali, per il tramite della Segreteria Tecnica, che riporta direttamente all'Amministratore delegato, tutti gli elementi necessari per avviare l'opportuno procedimento come parte attrice, allegando una nota istruttoria che illustri i motivi dell'azione e tutti i documenti di pertinenza.

L'Amministratore Delegato, di concerto con la Funzione Affari Legali e le altre funzioni interessate, nonché rimandando quando necessario al Consiglio di Amministrazione[29], valuta le possibili azioni da intraprendere, anche di natura transattiva, tenendo traccia delle motivazioni alla base delle decisioni assunte.

Nel caso in cui la gestione del contenzioso venga affidata ad un professionista esterno, la Funzione Legale Controllate, in coordinamento con la Funzione Risorse Umane presso la Capogruppo limitatamente ai contenziosi giuslavoristici, propone all'attenzione dell'Amministratore delegato della Capogruppo una rosa di possibili professionisti cui affidare l'incarico, indicando le motivazioni alla base della selezione effettuata, tra cui competenza, esperienza, continuità di azione e, ove possibile, omogenea ripartizione degli incarichi tra gli studi accreditati all'Albo dei fornitori legali della Capogruppo.

La Funzione Affari Legali, ovvero la Funzione Risorse Umane presso la Capogruppo limitatamente ai contenziosi giuslavoristici a seguito dell'incarico affidato al professionista designato, assicura:

- La tracciabilità di tutta la documentazione fornita al legale incaricato e delle azioni stabilite e ad esso comunicate;
- Il costante monitoraggio delle attività svolte e della strategia processuale posta in essere dal legale esterno, anche attraverso l'elaborazione, da parte del legale esterno, di una reportistica periodica relativa allo stato di avanzamento del processo.

Il Legale Controllate è tenuto ad inviare periodicamente, su base semestrale, all'Amministratore delegato un'informativa riepilogativa dei contenziosi in essere, con l'informazione relativa allo stato di avanzamento, al valore del contenzioso e al professionista incaricato.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate, la Funzione Legale controllate è tenuta alla comunicazione periodica, su base annuale, all'Organismo di Vigilanza ed al RPCT di un elenco dei contenziosi attivi e passivi avviati e di quelli conclusi con accordi transattivi, con indicazione dell'oggetto, del valore e del nominativo del professionista esterno incaricato (qualora applicabile).

In ogni caso, il responsabile dell'Ufficio Affari Legali presso la Capogruppo comunica all'OdV e al RPCT, con cadenza almeno annuale, le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

IV.3.2.2. Gestione dei rapporti con soggetti coinvolti in procedimenti innanzi all'autorità giudiziaria

Qualora un amministratore, un dirigente o un dipendente della Società sia chiamato - nella veste di indagato/imputato, persona informata sui fatti/testimone o teste assistito/imputato in procedimento - a rendere dichiarazioni innanzi all'Autorità Giudiziaria in merito ad attività connessa alla gestione e all'amministrazione societaria, è tenuto a mantenere il massimo riserbo in merito alle dichiarazioni rilasciate e al loro contenuto, ove le medesime siano coperte da segreto investigativo.

[29] In relazione ai poteri conferiti dal sistema di procure/deleghe in vigore

L'amministratore, il dirigente o il dipendente ha altresì l'obbligo di rigettare fermamente qualsiasi tentativo proveniente da altri soggetti interni o esterni alla Società, volto a condizionare il contenuto delle proprie dichiarazioni o a indurlo, qualora consentito dalla legge, ad avvalersi della facoltà di non rispondere. Qualora egli riceva indebite pressioni in tal senso o promesse di denaro o altre utilità volte al medesimo scopo, è tenuto ad informare immediatamente il proprio superiore gerarchico (o il soggetto a questi gerarchicamente sovraordinato qualora l'indebita pressione e la promessa di beni od utilità provenga dal proprio superiore gerarchico) e l'Organismo di Vigilanza nonché il RPCT per i provvedimenti di competenza.

Gli stessi principi, in quanto applicabili, sono osservati anche da terze parti interessate, in relazione alle dichiarazioni da rilasciare dinanzi all'Autorità Giudiziaria in merito a vicende di qualsiasi natura inerenti Infratel Italia di cui gli stessi siano a conoscenza.

A tutti i destinatari del Modello 231 - Parte Generale e Parte Speciale è fatto inoltre divieto di indurre chiunque, attraverso violenza o minaccia o tramite offerta o promessa di denaro o altre utilità, a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria al fine di favorire gli interessi della Società o per trarne altrimenti un vantaggio per la medesima.

In ogni caso, il responsabile dell'Ufficio Affari Legali presso la Capogruppo comunica all'OdV e al RPCT, con cadenza almeno annuale, le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

IV.4 SEGRETERIA SOCIETARIA

Infratel Italia assicura la formazione e l'attuazione delle decisioni degli Amministratori e Soci nel rispetto dei principi e delle prescrizioni contenute nelle disposizioni di legge vigenti, nell'atto costitutivo, nello statuto, nel Codice Etico, nel Modello 231, Parte Generale e Parte Speciale, e in altra regolamentazione di *governance* adottata dalla Società.

Gli Amministratori, il Collegio Sindacale, la Funzione Segreteria Societaria presso la Capogruppo, anche per tramite delle funzioni interne di supporto, e tutti i soggetti coinvolti nel processo in esame, sono tenuti a **non porre in essere atti o fatti che possano illecitamente determinare le delibere assembleari**, ad esempio inficiando la regolarità della convocazione, ammissione/intervento, votazione e verbalizzazione, omettendo o comunicando informazioni fuorvianti che possano viziare la volontà sociale.

La Segreteria Societaria presso la Capogruppo, anche per tramite delle funzioni interne di supporto in accordo alle sue politiche di governance, è tenuta a:

- **definire e dare comunicazione delle date** per i Consigli di Amministrazione e le Assemblee degli Azionisti;
- **predisporre**, sulla base delle indicazioni ricevute dai Soggetti titolati alla convocazione della riunione, **l'ordine del giorno** degli argomenti da discutere nel corso della stessa; tale ordine del giorno viene autorizzato mediante sottoscrizione dei Soggetti titolati quindi comunicato ai Consiglieri, ai Sindaci e alle funzioni aziendali interessate **dai provvedimenti in discussione**[30];
- **richiedere alle funzioni competenti la documentazione** necessaria alla presentazione in Consiglio/Assemblea degli argomenti definiti nell'ordine del giorno, quindi a **verificarne la coerenza**;
- **trasmettere**, tenendo traccia dell'avvenuto invio, la suddetta **documentazione ai Consiglieri/Soci**, con congruo anticipo rispetto alla data di riunione e comunque **entro i termini stabiliti** dalle Norme applicabili e dallo Statuto, al fine di consentire un'attenta analisi e di richiedere ulteriori informazioni prima della seduta. In particolare, deve essere assicurata la tempestiva messa a disposizione di tutti i componenti il Consiglio o

[30] Anche all'Organismo di Vigilanza in caso di adunanze Consiliari/Assembleari per l'approvazione di operazioni straordinarie

l'Assemblea della bozza di bilancio, corredata dalle relazioni del Collegio Sindacale e della Società di Revisione, prima della riunione per l'approvazione dello stesso;

- **archiviare e conservare la documentazione** relativa agli argomenti da trattare in Consiglio/Assemblea **per** permetterne la **consultazione ai soggetti autorizzati**;
- **archiviare e conservare tutta la documentazione rilevante e tutti gli atti**, l'ordine del giorno, le convocazioni, le delibere, i verbali delle riunioni e i libri sociali.

I Responsabili delle funzioni competenti assicurano completezza, correttezza, veridicità e aggiornamento della documentazione fornita e trasmessa alla Funzione Segreteria Societaria presso la Capogruppo, anche per tramite delle funzioni interne di supporto.

Le delibere del Consiglio inerenti all'approvazione di operazioni straordinarie[31] - tra cui l'acquisto di azioni proprie o della controllante, operazioni sul capitale, fusioni o scissioni - unitamente alle motivazioni delle operazioni stesse ed all'attestazione di avvenuta verifica di legittimità[32] delle operazioni in esame da parte degli organi amministrativi[33], **devono essere comunicate tempestivamente all'Organismo di Vigilanza.**

Qualora l'Assemblea sia chiamata a deliberare in merito ad operazioni straordinarie, **l'Organo Amministrativo predispone per l'Assemblea una relazione illustrativa delle operazioni in esame**. Detta relazione deve essere messa a disposizione dell'Assemblea con congruo anticipo rispetto alla data della riunione, comunque nel rispetto dei termini di legge ove applicabili, nonché **comunicata, entro detti termini, al Collegio Sindacale ed all'Organismo di Vigilanza.**

Gli Amministratori ed i Sindaci, laddove rivolgano comunicazioni o forniscano informazioni all'Assemblea, sono tenuti al rispetto dei criteri di attendibilità e completezza delle informazioni fornite.

La **verbalizzazione delle adunanze del Consiglio di Amministrazione avviene ad opera del Segretario nominato** dal Consiglio stesso; la **verbalizzazione delle risultanze dell'Assemblea dei Soci avviene a cura del Segretario nominato dalla stessa assemblea o dal notaio** designato nel caso di seduta straordinaria[34].
L'**Amministratore Delegato** di Infratel Italia, anche per il tramite della Funzione Segreteria Societaria presso la Capogruppo, è tenuto a **diffondere alle funzioni interessate** le informazioni pertinenti alle **deliberazioni assunte**.

La Funzione Segreteria Societaria presso la Capogruppo, anche per tramite delle funzioni interne di supporto, **rende disponibili** ai Soci, al Collegio Sindacale ed alla Società di Revisione le **informazioni e/o i documenti richiesti** dagli stessi e/o necessari per lo svolgimento delle attività di controllo loro deputate, garantendo il rispetto della normativa di riferimento (es. Codice civile) e tenendo traccia dell'accesso da parte dei suddetti organi.

Gli Amministratori comunicano tempestivamente al Consiglio di Amministrazione e al Collegio Sindacale tutte le informazioni relative alle cariche assunte o alle partecipazioni di cui sono titolari, direttamente o indirettamente, in altre società, nonché le cessazioni o le modifiche delle medesime le quali, per la natura o la tipologia, possono lasciar ragionevolmente prevedere **l'insorgere di conflitti di interesse**.

Gli Amministratori che, in occasione di una determinata operazione della Società, si trovino in una situazione **anche potenziale di conflitto di interessi** forniscono al Consiglio di Amministrazione adeguata informativa indicando la natura, i termini, l'origine e la portata del conflitto di interessi.

---

[31] Previo controllo di legittimità, ovvero di conformità dell'operazione alle prescrizioni di legge e di statuto nonché al rispetto sostanziale dei principi di corretta amministrazione sociale, da parte del Collegio Sindacale, il cui esito è oggetto di comunicazione agli Organi amministrativi, all'Assemblea e all'Organismo di Vigilanza

[32] Ovvero del rispetto dei dettami normativi applicabili alle operazioni in esame

[33] Anche sulla base di quanto verificato ed attestato dai soggetti e dalle funzioni competenti

[34] Le delibere Consiliari/Assembleari relative ad operazioni straordinarie sono oggetto di comunicazione tempestiva anche all'Organismo di Vigilanza

In relazione a qualsiasi tipo di attività aziendale, i Responsabili di funzione che riscontrino una situazione anche potenziale di conflitto di interessi, forniscono al Presidente/Amministratore Delegato e all'Organismo di Vigilanza adeguata informativa indicando la natura, i termini, l'origine e la portata del conflitto di interessi.

La Funzione Segreteria Societaria presso la Capogruppo, anche per tramite delle funzioni interne di supporto, tiene costantemente **aggiornato il sistema di procure e deleghe** di Infratel Italia e **comunica tempestivamente, ad ogni revisione**, le informazioni di pertinenza alle funzioni interessate e, con cadenza semestrale, all'Organismo di Vigilanza.

La *compliance* normativa è affidata all'unità Legale e Controllo Operativo interna, che di concerto con le funzioni interessate, analizza le problematiche legali e adotta le eventuali azioni correttive che non comportino l'insorgenza di un contenzioso (ad esempio in fase di gara, di acquisto o di recupero crediti). La funzione Legale di Capogruppo si coordina con il Controllo di Gestione e Recupero crediti per le attività prodromiche all'avvio del contenzioso relativo ai pagamenti insoluti.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate, la Funzione Segreteria Societaria presso la Capogruppo, anche per tramite delle funzioni interne di supporto, è tenuta alla comunicazione periodica, su base semestrale, all'Organismo di Vigilanza di un'informativa riepilogativa contenente l'ordine del giorno e la data di convocazione di tutte le riunioni di Infratel Italia indette nell'anno, la data di comunicazione ai convenuti e di deposito della documentazione, l'elenco della documentazione depositata.

In ogni caso, il responsabile dell'Ufficio Segreteria societaria presso la Capogruppo comunica all'OdV e al RPCT, con cadenza almeno annuale, le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

IV.5 SISTEMI INFORMATIVI

Sono affidate alla Capogruppo le attività relative al *Data Recovery; Desktop and Device Management; Identity and Access Management; Security and Networking; Server Management.*

Le attività a rischio (sensibili/strumentali) individuate in tale area sono relative alla gestione dei sistemi informativi: si tratta delle attività di pianificazione e organizzazione dei ruoli, delle risorse e delle attività connesse alla gestione dei sistemi informativi aziendali ed in particolare dei rischi informatici.

IV.5.1. ATTIVITÀ A RISCHIO E POTENZIALI REATI (SISTEMI INFORMATIVI)

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Gestione dei sistemi informativi	AD/Referente contratto di servizio Sistemi Informativi (Capogruppo)	Falsità in documento pubblico informatico; accesso abusivo a sistema informatico o telematico; detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici; intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche; detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche; detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche; danneggiamento di informazioni, dati e programmi informatici, anche utilizzati dallo Stato o altro ente pubblico o comunque di pubblica utilità; danneggiamento di sistemi informatici o telematici; detenzione, diffusione e installazione abusiva di	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 615-quater, 617-quater, 617.quinquies, 635-bis, 635-ter, 635-quater, 635-quater.1, 635-quinquies c.p.);** **Art. 25 d.lgs 231/2001 (artt. 318, 319, 320, 321, 322, 346-bis c.p.);** **Art. 25-novies d.lgs 231/2001 (art. 171, 171-bis, 171-ter, 174-sexies L. n. 633/1941)** **L. 190/2012 (artt. 334, 335 c.p.)** **RISCHIO STRUMENTALE:**

		apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico; danneggiamento di sistemi informatici o telematici di pubblico interesse; corruzione attiva e passiva; traffico di influenze illecite; istigazione alla corruzione; messa a disposizione del pubblico di un'opera dell'ingegno protetta o di parte di essa; duplicazione abusiva di programmi per elaboratore; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori; riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati; abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere scientifiche; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa; omessa segnalazione all'Autorità giudiziaria o alla P.G. di condotte penalmente rilevanti ai sensi della L. n. 633/1941, degli artt. 615-ter e 640-ter c.p.; Omessa comunicazione all'AGCOM un punto di contatto diretto; sottrazione o danneggiamento di cose sottoposte a sequestro; Violazione colposa di doveri inerenti alla custodia impedito controllo; impiego di cittadini di paesi terzi il cui soggiorno è irregolare paesi terzi il cui soggiorno è irregolare	**Art. 25-ter d.lgs 231/2001 (art. 2625 c.c.);** **Art. 25-duodecies d.lgs 231/2001 (art. 22, comma 12-bis, d.lgs n. 286/1998)**

IV.5.2. ELEMENTI DI CONTROLLO SISTEMI INFORMATIVI

Per le attività relative alla gestione dei sistemi informativi il Responsabile di processo coincide con la Funzione competente di Capogruppo, con l'Amministratore Delegato e con i Referenti interni a Infratel Italia per la gestione degli aspetti IT.
L'Amministratore Delegato e i Referenti interni garantiscono la piena conformità delle attività espletate dalla Capogruppo.

IV.5.2.1. Gestione dei Sistemi Informativi

La gestione dei sistemi informativi di Infratel Italia è curata dalla Capogruppo e regolamentata nell'ambito di opportuni contratti di outsourcing contenenti clausole di salvaguardia con riferimento, in particolare, alla sicurezza dei sistemi - nel rispetto delle politiche e degli elementi a presidio del rischio IT[35] stabiliti dal modello di organizzazione, gestione e controllo della Capogruppo ed anche declinati nel presente documento - ed al rispetto di specifici Service Level Agreement.

La Funzione Sistemi Informativi presso la Capogruppo, ovvero i Referenti interni responsabili della gestione di eventuali sistemi, applicativi e database proprietari o di terzi, assicurano:

- la corretta gestione IT dei sistemi attraverso la definizione di specifiche policies/procedure aziendali atte a disciplinare responsabilità e modalità operative per le diverse fasi di gestione di un progetto informatico, al fine di massimizzare l'efficacia e l'efficienza complessiva nonché minimizzare il rischio IT associato attraverso la definizione ed implementazione di opportuni requisiti di sicurezza;
- la corretta gestione delle infrastrutture tecnologiche a supporto delle applicazioni aziendali, nonché dei relativi dispositivi di sicurezza, anche attraverso la definizione e il monitoraggio di specifici piani di azione per l'acquisizione, il mantenimento, l'aggiornamento e la protezione di dette infrastrutture;

[35] Anche con riferimento a sistemi/apparecchiature fuori sede ed in relazione ai rischi connessi all'operare al di fuori del perimetro dell'organizzazione

- la progettazione e l'implementazione, ovvero l'acquisizione, delle applicazioni IT nel rispetto dei requisiti di business, opportunamente formalizzati dalla funzione richiedente, tenendo in considerazione i controlli applicativi e i necessari requisiti di sicurezza - autenticazione, gestione dei log, architettura applicativa;
- anche per il tramite delle funzioni competenti, l'acquisizione di sistemi e soluzioni da soggetti terzi previa formalizzazione di opportuni contratti di fornitura, in cui sono previste clausole di risoluzione e penali in relazione al mancato rispetto di specifici livelli di servizio e requisiti di sicurezza, nonché alla divulgazione delle informazioni proprietarie;
- la definizione, l'implementazione, la verifica e l'aggiornamento di un piano di continuità dei servizi IT, anche attraverso la conduzione di un'analisi sugli impatti aziendali e la valutazione dei rischi connessi, che prevede opportune soluzioni di *backup*, *recovery* e architetturali ad alta affidabilità;
- la confidenzialità, l'integrità, l'affidabilità e la disponibilità dei dati, delle informazioni e delle risorse IT attraverso la formalizzazione, la condivisione con le funzioni interessate e l'attuazione di un Piano di Sicurezza IT contenente le politiche, gli standard e le modalità operative specifiche per la certificazione delle soluzioni informatiche per gli aspetti di sicurezza, per il monitoraggio della stessa, lo svolgimento di test periodici e l'implementazione delle azioni correttive a fronte di punti di debolezza o incidenti identificati;
- l'identificazione univoca di tutti gli utenti e l'abilitazione delle relative identità attraverso opportuni meccanismi di autenticazione, l'assegnazione dei diritti di accesso ai sistemi e ai dati in linea con le necessità aziendali e le funzioni ricoperte. I diritti di accesso devono essere richiesti dai responsabili delle funzioni pertinenti, autorizzati dall'Amministratore del Sistema[36] e implementati dalla funzione responsabile della sicurezza informatica;
- l'individuazione delle regole e degli iter autorizzativi per la richiesta, la definizione, il rilascio, la sospensione, la modifica e la revoca, nonché per la revisione e il monitoraggio, degli identificativi utenti e i relativi privilegi, per i diversi sistemi e le applicazioni aziendali, per tutti gli utenti, inclusi quelli privilegiati quali gli Amministratori di Sistema;
- la definizione di responsabilità, modalità operative e flussi informativi per la gestione dei file di log prodotti dai sistemi informatici, ovvero per la generazione, registrazione, conservazione, estrazione nonché analisi e monitoraggio di detti file nei limiti consentiti, in accordo alle disposizioni legislative vigenti, al fine di avere disponibilità nel tempo delle informazioni significative inerenti l'utilizzo dei sistemi, tra le quali i soggetti che hanno avuto accesso, la tipologia e il momento in cui è stata compiuta una determinata azione e gli elementi/risorse interessate;
- la definizione di responsabilità e modalità operative da adottarsi per la registrazione, la classificazione e l'accesso a documenti informatici[37], anche al fine di valutare eventuali violazioni, modifiche non autorizzate, danni o perdite;
- la sicurezza fisica dei sistemi attraverso l'adozione di opportune modalità operative e misure di sicurezza adeguate per la protezione da accessi non autorizzati e da danneggiamento, anche accidentale;
- l'adozione di opportune misure anche preventive, sia organizzative sia tecniche, di rilevazione e correzione dei difetti del software, il monitoraggio periodico e il controllo puntuale del codice pericoloso (malware) al fine di garantire la protezione dei sistemi informativi e delle tecnologie da possibili rischi di sicurezza;
- l'utilizzo di procedure e tecniche di sicurezza (quali firewalls, dispositivi di sicurezza, segmentazione della rete e rilevazione delle intrusioni) per l'autorizzazione all'accesso e il controllo del flusso di informazioni da e per la rete aziendale;
- la qualità, tempestività e disponibilità dei dati di business attraverso l'adozione di procedure efficaci per la gestione delle librerie dei supporti di memorizzazione, il salvataggio e il ripristino dei dati.

I Referenti interni, anche avvalendosi della collaborazione degli uffici interni responsabili della Privacy,

[36] Amministratori di Sistema nominati nel rispetto del provvedimento del Garante della Privacy del 27 novembre 2008 in tema di "Misure ed accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"

[37] Ovvero qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli

opportunamente identificati dall'Amministratore Delegato e/o dai Soggetti titolati della Società, assicurano il monitoraggio periodico:

- della corretta implementazione dei presidi tecnico/operativi anche stabiliti nell'ambito del servizio di outsourcing;
- dell'efficacia dei presidi tecnici/operativi riferiti all'adozione delle misure minime di cui al Disciplinare Tecnico Allegato B del D.Lgs. 196/2003 e successive modifiche.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate, la Funzione Sistemi Informativi presso la Capogruppo è tenuta alla comunicazione periodica, su base annuale, all'Amministratore Delegato, all'OdV e al RPCT di un'informazione riepilogativa di tutti gli interventi sul sistema informativo effettuati nel periodo, con indicazione della tipologia di intervento, dell'Ufficio/Funzione richiedente, della cause che hanno reso necessario l'intervento, del tipo di iter seguito e di eventuali spese legate alla realizzazione dell'intervento, anche specificando gli eventuali rapporti accertati con fornitori/partner commerciali della Società

In ogni caso, il responsabile dell'Ufficio Sistemi Informativi presso la Capogruppo comunica all'OdV e al RPCT, con cadenza almeno annuale, le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

IV.6 AMMINISTRAZIONE E BILANCIO

Sono affidate alla Capogruppo le attività relative alla Governance Controllate e al Service Amministrativo.

IV.6.1. ATTIVITÀ A RISCHIO E POTENZIALI REATI (AMMINISTRAZIONE E BILANCIO)

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Predisposizione di bilanci e relazioni e comunicazioni sociali	Resp. funzione Capogruppo/ A.D.	False comunicazioni sociali; False comunicazioni sociali delle società quotate; impedito controllo dei soci o organi sociali; indebita restituzione di conferimenti; illegale ripartizione degli utili e delle riserve; illecite operazioni sulle azioni o quote sociali o della società controllante; operazioni in pregiudizio dei creditori; omessa comunicazione del conflitto d'interessi; formazione fittizia del capitale; indebita ripartizione dei beni sociali da parte dei liquidatori; corruzione tra privati; istigazione alla corruzione tra privati; illecita influenza sull'assemblea; aggiotaggio; Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; concussione; corruzione attiva o passiva di pubblico ufficiale o incaricato di pubblico servizio; corruzione in atti giudiziari; induzione indebita a dare o promettere utilità; istigazione alla corruzione; induzione indebita a dare o promettere utilità, corruzione attiva e passiva, corruzione in atti giudiziari, istigazione alla corruzione - di membri degli organi UE o di funzionari UE; traffico di influenze illecite; manipolazione del mercato; ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita; autoriciclaggio; dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti;	**RISCHIO DIRETTO:** **Art. 25-ter d.lgs 231/2001 (artt. 2621, 2622, 2625, 2626, 2627, 2628, 2629, 2629 bis, 2632, 2633, 2635, 2635 bis, 2636, 2637, 2638 c.c.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 640, 640-bis c.p.);** **Art. 25 d.lgs 231/2001;** **Art. 25-sexies d.lgs 231/2001 (art. 185 TUF);** **Art. 25-octies d.lgs 231/2001;** **Art. 25-quinquiesdecies (artt. 2, 3, 8, 10, 11 d.lgs n. 74/2000)**

		dichiarazione fraudolenta mediante altri artifici; emissione di fatture o altri documenti per operazioni inesistenti; occultamento o distruzione di documenti contabili; sottrazione fraudolenta al pagamento di imposte	
Gestione degli aspetti fiscali	A.D./Resp. funzione capogruppo	Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti; dichiarazione fraudolenta mediante altri artifici; emissione di fatture o altri documenti per operazioni inesistenti; occultamento o distruzione di documenti contabili; sottrazione fraudolenta al pagamento di imposte; ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita; autoriciclaggio; Sottrazione all'accertamento o al pagamento dell'accisa sugli prodotti energetici	**RISCHIO DIRETTO:** **Art. 25-quinquiesdecies d.lgs 231/2001 (artt. 2, 3, 8, 10, 11 d.lgs. n. 74/2000)** **RISCHIO STRUMENTALE:** **Art. 25-octies d.lgs 231/2001;** **Art. 25-sexiesdecies d.lgs 231/2001 (art. 40 d.lgs 504/1995, comma 1, lett.c))**

Gestione della tesoreria, finanza e crediti (gestione dei conti correnti, incassi, pagamenti e finanza di proprietà); gestione crediti; gestione investimenti in strumenti finanziari; gestione dei buoni pasto	A.D./Resp. funzione capogruppo	Malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; frode nelle pubbliche forniture; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; concussione; corruzione attiva o passiva; corruzione in atti giudiziari; induzione indebita a dare o promettere utilità; istigazione alla corruzione; induzione indebita a dare o promettere utilità, corruzione attiva e passiva, corruzione in atti giudiziari e istigazione alla corruzione di membri degli organi UE o di funzionari UE; traffico di influenze illecite; alterazione di carte di pubblico credito; falsificazione, spendita e introduzione nello Stato di carte di pubblico credito falsificate; falsificazione, detenzione, uso e messa in circolazione di valori di bollo falsificati; contraffazione, alterazione o uso di marchi o segni distintivi di prodotti industriali ovvero di brevetti, disegni o modelli industriali; introduzione nello Stato e commercio di prodotti con segni falsi; ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita; autoriciclaggio; indebito utilizzo e falsità in strumenti di pagamento diversi dai contanti; detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti; trasferimento fraudolento di valori; rifiuto d'atti d'ufficio. omissione turbata libertà degli incanti; turbata libertà del procedimento di scelta del contraente; false comunicazioni sociali; false comunicazioni sociali delle società quotate; impedito controllo dei soci o organi sociali; indebita restituzione di conferimenti; illegale ripartizione degli utili e delle riserve; illecite operazioni sulle azioni o quote sociali o della società controllante; operazioni in pregiudizio dei creditori; omessa comunicazione del conflitto d'interessi; formazione fittizia del capitale; indebita ripartizione dei beni sociali da parte dei liquidatori; corruzione tra privati; istigazione alla corruzione tra privati; illecita influenza sull'assemblea; aggiotaggio; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti; dichiarazione fraudolenta mediante altri artifici; emissione di fatture o altri documenti per operazioni inesistenti; occultamento o distruzione di documenti contabili; sottrazione fraudolenta al pagamento di imposte	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 640, 640-bis, 640-ter, 356 c.p.);** **Art. 25 d.lgs. 231/2001;** **Art. 25-bis d.lgs. 231/2001 (artt. 453, 454, 455, 457, 458, 459, 464, 473, 474 c.p.);** **Art. 25-octies, d.lgs 231/2001;** **Art. 25-octies.1 d.lgs 231/2001 (artt. 493-ter, 493-quater, 512-bis c.p.)** **L. 190/2012 (art. 328 c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 353, 353-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2621, 2622, 2625, 2626, 2627, 2628, 2629, 2629 bis, 2632, 2633, 2635, 2635 bis, 2636, 2637, 2638 c.c.);** **Art. 25-quinquesdecies d.lgs 231/2001 (artt. 2, 3, 8, 10, 11 d.lgs n. 74/2000)**

Fatturazione attiva	A.D./Resp. funzione capogruppo	Emissione di fatture o altri documenti per operazioni inesistenti; Malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; frode nelle pubbliche forniture; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; concussione; corruzione attiva o passiva; corruzione in atti giudiziari; induzione indebita a dare o promettere utilità; istigazione alla corruzione; induzione indebita a dare o promettere utilità, corruzione attiva e passiva, corruzione in atti giudiziari e istigazione alla corruzione di membri degli organi UE o di funzionari UE; traffico di influenze illecite; false comunicazioni sociali; false comunicazioni sociali delle società quotate; impedito controllo dei soci o organi sociali; corruzione tra privati; istigazione alla corruzione tra privati; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita; autoriciclaggio; dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti; dichiarazione fraudolenta mediante altri artifici; emissione di fatture o altri documenti per operazioni inesistenti	**RISCHIO DIRETTO:** **Art. 25-quinquiesdecies d.lgs 231/2001 (art. 8 d.lgs n. 74/2000)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 640, 640-bis, 640-ter, 356 c.p.);** **Art. 25 d.lgs. 231/2001;** **Art. 25-ter d.lgs 231/2001 (artt. 2621, 2622, 2625, 2635, 2635 bis, 2638 c.c.);** **Art. 25-octies d.lgs 231/2001;** **Art. 25-quinquesdecies d.lgs 231/2001 (artt. 2, 3, 8 d.lgs 74/2000)**

IV.6.2. ELEMENTI DI CONTROLLO AMMINISTRAZIONE E BILANCIO

Per le attività relative all'Amministrazione e Bilancio, il Responsabile di processo coincide con la Funzione competente di Capogruppo, con il Referente di Contratto di Servizio/Amministratore Delegato e con i Referenti interni Infratel Italia per la gestione degli aspetti amministrativi e del recupero crediti.
Il Referente di Contratto di Servizio/Amministratore Delegato garantisce il rispetto delle attività espletate dalla Capogruppo.

IV.6.2.1. Predisposizione di bilanci, relazioni e comunicazioni sociali/gestione della contabilità generale e formazione del bilancio civilistico

Infratel Italia assicura correttezza, trasparenza, veridicità e tracciabilità nella conduzione delle attività per la tenuta della contabilità e la formazione del bilancio, nel rispetto delle normative vigenti, delle disposizioni applicabili in materia di bilancio consolidato, degli standard/policy della Capogruppo.

Gli Amministratori, la Funzione Service Amministrazione e Bilancio presso la Capogruppo, nonché le altre funzioni interne interessate e competenti, assicurano, in tutte le attività preordinate alla formazione dei documenti contabili societari anche finalizzate alla redazione del bilancio, ovvero nelle comunicazioni/resoconti sociali, un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società.

Ai suddetti soggetti è fatto divieto di rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni, prospetti o altre comunicazioni sociali, dati falsi, volutamente lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della Società, nonché omettere dati e informazioni necessari per adempiere alle obbligazioni societarie rilevanti.

La Funzione Amministrazione e Bilancio presso la Capogruppo assicura:

- che le scritture e le registrazioni contabili siano effettuate in modo da riflettere accuratamente e correttamente tutte le operazioni della Società;
- che tutti i costi e oneri, i ricavi e proventi, gli incassi e gli esborsi siano rappresentati in contabilità in modo veritiero e corretto, opportunamente documentati in conformità alla legislazione vigente;

- che ogni rilevazione o registrazione relativa a operazioni di natura straordinaria sia supportata da idonea documentazione predisposta dalla funzione interna competente;
- l'organizzazione delle attività da svolgere secondo un calendario di chiusura determinato dai vertici aziendali, individuando i responsabili e le tempistiche rilevanti per la trasmissione dei dati amministrativo-contabili da parte delle funzioni interne competenti, necessari alla produzione e trasmissione del bilancio anche alle funzioni preposte della Capogruppo, ai fini dell'elaborazione del consolidato, delle relazioni e delle altre comunicazioni sociali richieste dalla legge.

La rilevazione delle informazioni contabili avviene anche per il tramite di sistemi e applicazioni informatiche a garanzia della tracciabilità dei singoli passaggi del processo di formazione dei dati. I profili di accesso a tali sistemi assicurano la separazione delle funzioni e la coerenza dei livelli autorizzativi.

La Funzione Sistemi Informativi presso la Capogruppo è responsabile del processo di verifica e manutenzione dei suddetti sistemi o applicazioni informatiche con riferimento, in particolare, alla salvaguardia e protezione dei dati e delle informazioni nel rispetto delle policies/procedure interne emanate in materia di tutela del patrimonio informativo aziendale.

Le funzioni interne interessate assicurano, nel rispetto dei tempi e delle modalità prestabilite, la trasmissione alla Funzione Amministrazione presso la Capogruppo dei dati e delle informazioni di competenza, attraverso opportune comunicazioni formali sottoscritte dal responsabile di funzione interno o, laddove previsto, per il tramite di un sistema informatico, a cui allegano la documentazione pertinente e di supporto alle valutazioni/stime delle poste di rettifica nonché una lettera di attestazione di veridicità e completezza delle informazioni trasferite.

È fatto obbligo generale e diffuso di riferire tempestivamente alla Funzione Amministrazione presso la Capogruppo ogni notizia ed informazione relativa ad errori, distorsioni informative od omissioni nel contesto della predisposizione di comunicazioni sociali.

La Funzione Amministrazione e Bilancio presso la Capogruppo, di concerto con le funzioni interne competenti, provvede al recepimento di dati/informazioni ricevute effettuando opportuni controlli di coerenza, quadrature e riconciliazioni con i dati disponibili e i saldi contabili. Qualora siano riscontrati disallineamenti o siano apportate variazioni rispetto a quanto comunicato dalle funzioni competenti, le necessarie rettifiche devono essere condivise con le funzioni stesse e le funzioni di controllo interessate.

Il progetto di bilancio, predisposto dalla Funzione Amministrazione e Bilancio presso la Capogruppo in collaborazione con le altre funzioni interne per le parti di competenza, deve essere verificato dal Responsabile della Funzione Amministrazione e Bilancio presso la Capogruppo e successivamente sottoposto all'approvazione del Presidente/Amministratore Delegato di Infratel Italia[38].

La Funzione Amministrazione e Bilancio presso la Capogruppo assicura correttezza, trasparenza e tracciabilità nella gestione dei rapporti con il Collegio Sindacale e con la Società di Revisione nell'ambito delle attività di controllo ad essi demandate ai sensi della normativa in materia, con riferimento, in particolare, all'analisi ed alla verifica del progetto di bilancio nonché delle informazioni amministrative, contabili e finanziarie, ad esso correlate o strumentali alla corretta gestione degli adempimenti fiscali della Società[39].

Preventivamente all'approvazione del bilancio sono effettuati incontri tra il Collegio Sindacale, la Società di Revisione e l'Organismo di Vigilanza.

[38] In relazione ai poteri conferiti dal sistema di procure/deleghe in vigore

[39] In particolare, deve essere tenuta traccia delle richieste ricevute nonché delle informazioni/documentazione fornita

La Funzione Amministrazione e Bilancio presso la Capogruppo è tenuta alla conservazione e all'archiviazione, secondo modalità atte a garantirne la riservatezza e la protezione da accessi non autorizzati, della documentazione amministrativo contabile nel rispetto dei termini normativi applicabili[40].

Fermo restando l'obbligo in capo a tutti gli attori coinvolti di comunicare eventuali anomalie o atipicità riscontrate, la Funzione Amministrazione presso la Capogruppo è tenuta a comunicare all'Organismo di Vigilanza e al RPCT, ogni osservazione formulata sia dalla Società di Revisione sia dal Collegio Sindacale[41], nonché l'esito di eventuali accertamenti o contestazioni da parte dell'Amministrazione Finanziaria, periodicamente, su base annuale, un'informativa riepilogativa, evidenziando in particolare eventuali altri incarichi affidati da Infratel Italia alla società incaricata della revisione del bilancio a società ad essa collegate[42].

In ogni caso, il responsabile dell'Ufficio Amministrazione e Bilancio presso la Capogruppo comunica all'OdV e al RPCT, con cadenza almeno annuale, le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

IV.6.2.2. Gestione degli aspetti fiscali

Infratel Italia assicura, anche in collaborazione con gli uffici preposti di Capogruppo, che le attività inerenti la gestione degli aspetti fiscali siano condotte in maniera corretta, trasparente e tracciabile, nel rispetto della normativa vigente e applicabile alla Società;

La Funzione Amministrazione e Bilancio presso la Capogruppo, anche in collaborazione o per il tramite degli uffici interni preposti[43], sulla base del processo di gestione della contabilità generale e di formulazione del bilancio[44], assicura il corretto assolvimento degli obblighi normativi in materia di dichiarazioni periodiche relative alle imposte dirette e indirette, nonché del pagamento delle imposte (es. imposta sul valore aggiunto, ritenute certificate, contributi del personale), ad eccezione delle dichiarazioni e certificazioni relative ai dipendenti demandata alla Funzione Risorse Umane - Amministrazione del Personale della Capogruppo.

La Funzione Amministrazione e Bilancio presso la Capogruppo, nel rispetto dei termini di legge, assicura la tempestiva comunicazione/trasmissione delle suddette dichiarazioni agli organi preposti, anche per il tramite di studi legali/tributari esterni, nonché il tempestivo pagamento dei suddetti modelli, in accordo alle modalità previste dalla normativa applicabile.

La Funzione Amministrazione e Bilancio presso la Capogruppo provvede altresì alla comunicazione periodica, almeno su base semestrale, verso l'Amministratore Delegato e l'Organismo di Vigilanza, di una reportistica di sintesi degli adempimenti fiscali ottemperati nel periodo di riferimento[45].

---

[40] Anche attraverso l'utilizzo di applicazione informatiche in possesso di opportuni requisiti di sicurezza, in accordo agli elementi di controllo stabiliti per il processo di gestione dei Sistemi Informativi

[41] Con riferimento ad eventuali problematiche emerse in relazione al progetto di bilancio, o più in generale alla corretta applicazione dei principi contabili

[42] Previa richiesta di informazione alle funzioni competenti

[43] I rapporti di collaborazione tra Infratel Italia e la Capogruppo, con riferimento alla gestione di specifici aspetti fiscali, sono regolamentati nell'ambito del contratto di servizio in essere, contenente opportune clausole di salvaguardia con riferimento, in particolare, alla corretta esecuzione delle attività di predisposizione delle dichiarazioni/modelli relativi alle ritenute certificate del personale dipendente e assimilato, nel rispetto delle modalità e dei termini previsti dalle normative applicabili in materia fiscale

[44] Anche supportato da sistemi informatici gestionali atti all'implementazione di meccanismi automatici di corretta contabilizzazione (es. automatica alimentazione dei registri iva)

[45] Modelli di dichiarazione e quietanze di pagamento

La Funzione Amministrazione[46] è tenuta alla conservazione e archiviazione della documentazione amministrativo contabile inerente la gestione degli aspetti fiscali, nel rispetto dei termini normativi applicabili.

La Funzione Amministrazione presso la Capogruppo assicura, in presenza dell'Amministratore Delegato e/o dei soggetti dallo stesso incaricati, correttezza, trasparenza e tracciabilità nella gestione dei rapporti con le autorità e gli organi di vigilanza e controllo in materia di adempimenti fiscali (es. Guardia di Finanza, Agenzia delle Entrate), con riferimento, in particolare, all'analisi e alla verifica della gestione degli adempimenti in materia da parte della Società[47], nel rispetto degli elementi di controllo declinati nel presente Modello 231 - Parte Speciale e relativi al processo di gestione degli adempimenti[48], delle comunicazioni e delle relazioni con le autorità pubbliche e altri organi di vigilanza e controllo, anche in occasione di verifiche ispettive.

In ogni caso, il responsabile dell'Ufficio Amministrazione e Bilancio presso la Capogruppo comunica all'OdV e al RPCT, con cadenza almeno annuale, le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

IV.7 GESTIONE DELLA TESORERIA, FINANZA E CREDITI

IV.7.1. GESTIONE CONTI CORRENTI, INCASSI, PAGAMENTI E FINANZA DI PROPRIETÀ

Fermo restando eventuali specifiche modalità stabilite dagli accordi o convenzioni stipulate da Infratel Italia con la Pubblica Amministrazione, la Società assicura il rispetto di tutti gli obblighi normativi applicabili in materia di prevenzione del riciclaggio e antimafia con riferimento alle modalità di esecuzione dei pagamenti/incassi e delle transazioni finanziarie.

L'istituzione di nuovi rapporti o la dismissione di rapporti in essere con istituti bancari o finanziari è autorizzata dall'Amministratore Delegato, all'esito di un'opportuna analisi sulla competitività di detti istituti di credito selezionati.

Le operazioni di apertura/chiusura conti correnti, nonché la destinazione dei fondi in essi contenuti, la richiesta di fidi, fidejussioni e altre operazioni anche di natura straordinaria sono autorizzate dall'Amministratore Delegato.

Periodiche attività di riconciliazione bancaria e di monitoraggio conti sono assicurate dalla Funzione Amministrazione presso la Capogruppo che provvede alla tempestiva comunicazione, ai soggetti interessati, di eventuali anomalie o discordanze riscontrate per la definizione di opportune azioni da porre in essere.

La Funzione Amministrazione presso la Capogruppo assicura, in collaborazione con le funzioni interne competenti, prima della disposizione di pagamento oggetto di autorizzazione finale da parte dei Soggetti titolati della Società in accordo al sistema di procure e deleghe vigente:

- la verifica della regolarità fiscale della fattura;
- la verifica di affidabilità/onorabilità dell'istituto di credito utilizzato dal soggetto creditore - appartenenza a Stati segnalati come non cooperativi o a regimi fiscali agevolati secondo le indicazioni di organismi nazionali e/o sopranazionali operanti nell'antiriciclaggio e nella lotta al terrorismo - nonché di corrispondenza del conto

[46] Anche per il tramite degli uffici competenti di Capogruppo, in accordo al contratto di servizio in essere

[47] In particolare, deve essere tenuta traccia delle richieste ricevute da detti organi di controllo nonché delle informazioni/documentazione ad essi fornita

[48] Al fine di mitigare il rischio fiscale, la Società si avvale, ove possibile, di procedure di cooperative compliance fiscale, interpello e quanto altro consentito dai codici in ordine alla definizione dei tributi dovuti.

corrente di accredito con quello dedicato, laddove applicabile ai sensi della normativa di riferimento, comunicato formalmente in corso di gestione del rapporto;

- la presenza di tutte le firme autorizzative dei Soggetti titolati, in relazione all'importo in accordo al sistema di procure e deleghe in essere;
- la verifica di regolare esecuzione della prestazione e degli importi da corrispondere anche attraverso la rilevazione della documentazione attestante l'avvenuta fornitura/prestazione opportunamente autorizzata dal referente interno di riferimento, identificato quale responsabile di contratto o del soggetto creditore;
- la comunicazione alle funzioni interessate ed all'Amministratore Delegato di eventuali anomalie riscontrate, nonché alla Funzione Legale della Capogruppo ed all'Organismo di Vigilanza, qualora opportuno, anche in relazione alla frequenza e alla tipologia degli elementi anomali rilevati, per la definizione e l'attuazione di adeguate azioni preliminari alla disposizione di pagamento.

La conservazione e archiviazione delle fatture avviene automaticamente attraverso lo SDI ed evidenza dei bonifici effettuati è raccolta tramite l'home banking dell'istituto di credito utilizzato[49].

Il mancato pagamento, ovvero il ripetuto ritardato pagamento di soggetti creditori, deve essere opportunamente motivato dalla Funzione Amministrazione presso la Capogruppo, in relazione alle indicazioni ricevute dal referente di contratto di riferimento e dai Soggetti titolati.

Le modalità di pagamento utilizzate sono solo quelle consentite dalla normativa vigente atte a garantire la tracciabilità dell'operazione svolta ovvero dell'importo, mittente, destinatario e causale[50]. Non sono ammesse operazioni in contanti, eccetto pagamenti per piccola cassa, consentiti per spese minute di importo massimo predefinito e stabilito nel rispetto dei limiti di legge. La Funzione Amministrazione e Bilancio presso la Capogruppo è inoltre responsabile della gestione della cassa di sede ed è tenuta ad effettuare periodicamente un'attività di monitoraggio sulla giacenza/movimentazione della stessa (di cui si rimanda all'istruzione operativa di riferimento).

In riferimento ai processi che generano fatturazione attiva, la Funzione Amministrazione presso la Capogruppo, in collaborazione con le funzioni interne competenti, assicura:

- l'emissione della fattura previa verifica dei documenti di riferimento, relativi ai processi che originano la fatturazione attiva (e.g. ordine di vendita/fatturazione), quindi la registrazione contabile e l'aggiornamento dello scadenziario crediti[51];
- per qualsiasi entrata di denaro, la verifica di corrispondenza dell'incasso con i relativi documenti di ciclo attivo, nonché la verifica che non sussistano elementi di anomalia in termini di provenienza dell'incasso, mittente non corrispondente, istituto di credito non affidabile, mancata corrispondenza del pagamento con la fattura emessa. Qualora un incasso non sia immediatamente riconducibile a un credito rilevato in contabilità, la Funzione Amministrazione e Bilancio presso la Capogruppo provvede a rilevare l'operazione[52], in attesa dell'identificazione della stessa, con il supporto delle funzioni coinvolte e il coinvolgimento dell'Amministratore Delegato;
- la comunicazione alle funzioni interessate e all'Amministratore Delegato di eventuali anomalie rilevate, nonché alla Funzione Affari Legali presso la Capogruppo e all'Organismo di Vigilanza, qualora opportuno, anche in relazione alla frequenza e alla tipologia degli elementi anomali rilevati per la definizione e l'attuazione di

[49] Amministrazione è tenuta a conservare ed archiviare anche i documenti corrispondenti di ciclo attivo

[50] Le operazioni tramite "home banking" possono essere effettuate solamente dai soggetti opportunamente delegati/titolati, previo riscontro dell'esecuzione delle verifiche prodromiche all'esecuzione del pagamento sopra definite

[51] Amministrazione assicura correttezza, veridicità e completezza dei dati e delle informazioni oggetto di fatturazione, nel rispetto delle norme nazionali ed europee nonché degli accordi formali applicabili

[52] Anche attraverso l'utilizzo di conti transitori e comunque assicurando la movimentazione delle somme connesse solo a valle dell'identificazione dell'operazione e/o della definizione di opportune azioni correttive in caso di anomalie accertate.

adeguate azioni correttive. Le opportunità di investimento/disinvestimento[53] sono determinate dalla Funzione Amministrazione e Bilancio presso la Capogruppo; quindi, autorizzate dai Soggetti titolati della Società[58], previa informativa al Consiglio di Amministrazione.

La Funzione Amministrazione e Bilancio presso la Capogruppo assicura la gestione della custodia degli eventuali titoli della Società, disponendo eventuali trasferimenti tra conti, previa autorizzazione da parte dei Soggetti titolati della Società[54].

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate, la Funzione Amministrazione e Bilancio presso la Capogruppo è tenuta alla comunicazione periodica, su base semestrale, all'Organismo di Vigilanza e al RPCT di un'informativa riepilogativa delle anomalie riscontrate nelle fase di incasso e pagamento con indicazione delle azioni intraprese, delle operazioni di chiusura dei conti correnti e destinazione dei relativi fondi, delle operazioni d'investimento/disinvestimento effettuate nel periodo di riferimento.

In ogni caso, il responsabile dell'Ufficio Amministrazione e Bilancio presso la Capogruppo comunica all'OdV e al RPCT, con cadenza almeno annuale, le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

IV.7.2. GESTIONE CREDITI

Infratel Italia assicura che il processo di gestione dei crediti sia condotto in maniera corretta, trasparente e tracciabile, nel modo più tempestivo ed efficace possibile, anche al fine di assicurare adeguata e tempestiva informazione circa le previsioni di incasso, l'insorgenza di morosità e lo stato delle procedure di recupero di eventuali crediti scaduti.

Con le attività di recupero crediti si assicura:

- l'aggiornamento costante dello scadenzario crediti, coerentemente alla situazione contabile, nei confronti dei debitori rilevata dalla Funzione Amministrazione e Bilancio presso la Capogruppo, tenuta alla corretta imputazione e alla tempestiva registrazione delle singole partite di credito e dei relativi incassi;
- la predisposizione periodica della situazione riepilogativa dei crediti scaduti, oggetto di comunicazione alle funzioni interessate, anche al fine di ottenere indicazioni relative alle possibili cause di mancato pagamento;
- alla scadenza di ciascun credito, la gestione delle problematiche del mancato incasso verso il soggetto debitore, previa condivisione con le funzioni titolate della Società, anche attraverso l'emissione di una o più comunicazioni formali di sollecito;
- qualora non si sia verificato l'incasso nei termini stabiliti, sentito il parere della funzione interessata e della Funzione Affari Legali presso la Capogruppo, l'attivazione di possibili soluzioni alternative, previa verbalizzazione delle motivazioni alla base dell'azione stabilita, da sottoporre all'Amministratore Delegato per approvazione, quali la definizione di piani di rientro e/o consolidamento del credito, il ricorso al recupero coattivo, la cancellazione dei crediti per i quali le azioni legali non risultino economicamente convenienti;
- nel caso di recupero coattivo del credito, la comunicazione formale alla Funzione Affari Legali presso la Capogruppo di tutta la documentazione pertinente attestante la posizione creditoria e le azioni già poste in essere per il recupero del credito.

La Funzione Affari Legali presso la Capogruppo assicura:

[53] Sono previste solo operazioni di accantonamento di natura non speculativa con operatori finanziari di riconosciuta affidabilità e onorabilità

[54] In funzione dell'importo in accordo al sistema di procure e deleghe in vigore

- la predisposizione e la comunicazione formale delle lettere di diffida ai soggetti debitori nonché, qualora necessario, l'attivazione del contenzioso;
- la comunicazione periodica, su base semestrale, alla Funzione interna Recupero Crediti e alla Funzione Amministrazione presso la Capogruppo, di una situazione riepilogativa dei crediti in contenzioso, indicativa dei soggetti coinvolti, della natura e dell'importo, del tipo di azione intrapresa e del relativo stato, delle possibilità di recupero del credito.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate, la Funzione Amministrazione presso la Capogruppo è tenuta alla comunicazione periodica, su base semestrale, all'Organismo di Vigilanza ed al RPCT di un'informativa riepilogativa dei crediti scaduti[55]

In ogni caso, il responsabile dell'Ufficio Affari Legali presso la Capogruppo comunica all'OdV e al RPCT, con cadenza almeno annuale, le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

IV.8 RISORSE UMANE

Sono affidate alla Capogruppo le attività relative alla organizzazione e sviluppo risorse umane, gestione risorse umane e relazioni industriali, amministrazione del personale.

IV.8.1. ATTIVITÀ A RISCHIO E POTENZIALI REATI (RISORSE UMANE)

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Selezione e assunzione del personale	AD/ufficio interessato, Risorse Umane (Capogruppo) /Referente contratto di servizio	Corruzione attiva e passiva; corruzione in atti giudiziari; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione tra privati, istigazione alla corruzione tra privati; intermediazione illecita e sfruttamento del lavoro; omicidio colposo e lesioni personali gravi o gravissime colpose commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro; induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria; impiego di cittadini di paesi terzi il cui soggiorno è irregolare; malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; condotte favorenti l'immigrazione clandestina	**RISCHIO DIRETTO:** **Art. 25 d.lgs 231/2001 (artt. 318, 319, 319-ter, 319-quater; 320, 322, 346-bis cp);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 263-bis cc);** **Art. 25-quinquies d.lgs 231/2001 (art. 603 bis cp);** **Art. 25-septies d.lgs 231/2001;** **Art. 25-decies d.lgs 231/2001 (art. 377-bis cp);** **Art. 25-duodecies d.lgs. 231/2001 (art. 22 comma 12-bis d.lgs. n. 286/1998)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 640, 640-bis c.p.);** **Art. 25 d.lgs 231/2001 (artt. 317, 318, 319, 319-quater, 322 c.p.);** **Art. 25-duodecies d.lgs. 231/2001 (art. 12, commi 3, 3-bis, 3-ter e 5 d.lgs n. 286/1998)**

[55] Eventualmente allegando le note ricevute dalle funzioni interessate

Impiego di personale di paesi terzi	AD/ufficio interessato, Risorse Umane (Capogruppo) /Referente contratto di servizio	Intermediazione illecita e sfruttamento del lavoro; impiego di cittadini di paesi terzi il cui soggiorno è irregolare; condotte favorenti l'immigrazione clandestina; malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche	**RISCHIO DIRETTO:** **Art. 25-quinquies d.lgs 231/2001 (art. 603 bis cp);** **Art. 25-duodecies d.lgs. 231/2001 (artt. art. 12, commi 3, 3-bis, 3-ter, 5, e 22, comma 12-bis, d.lgs. n. 286/1998)** **Rischio strumentale:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 640, 640-bis c.p.);**
Sviluppo e incentivazione delle risorse	AD/ufficio interessato, Risorse Umane (Capogruppo) /Referente contratto di servizio	Falsità in documento pubblico informatico; corruzione attiva e passiva; corruzione in atti giudiziari; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione tra privati, istigazione alla corruzione tra privati; ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita; autoriciclaggio; malversazione di erogazioni pubbliche truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; intermediazione illecita e sfruttamento del lavoro; omicidio colposo e lesioni gravi o gravissime colpose - commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro; Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (art. 491-bis c.p.);** **Art. 25 d.lgs. 231/2001 (artt. 318, 319, 319-ter, 319-quater; 320, 321, 322, 346-bis cp);** **Art. 25-ter (art. 2635, 2635-bis cc);** **Art. 25-octies d.lgs 231/2001;** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 640, 640-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis c.c.);** **Art. 25-quinquies (art. 603 bis c.p.);** **Art. 25-septies d.lgs. 231/2001;** **Art. 25-decies (art. 377-bis c.p.)**
Formazione	AD/ufficio interessato, Risorse Umane (Capogruppo) /Referente contratto di servizio	Falsità in documento pubblico informatico; accesso abusivo a sistema informatico o telematico; intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche; danneggiamento di informazioni, dati e programmi informatici, anche utilizzati dallo Stato o altro ente pubblico o comunque di pubblica utilità; danneggiamento di sistemi informatici o telematici; danneggiamento di sistemi informatici o telematici di pubblico interesse; omicidio colposo e lesioni gravi o gravissime colpose - commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro; messa a disposizione del pubblico di un'opera dell'ingegno protetta o di parte di essa; duplicazione abusiva di programmi per elaboratore; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori; riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati; abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere scientifiche; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa; omessa segnalazione alla Autorità giudiziaria o alla P.G. di condotte penalmente rilevanti ai sensi della L. n. 633/1941, degli artt. 615-ter e 640-ter c.p.; omessa comunicazione all'AGCOM di un punto di contatto diretto	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 617-quater, 635-bis, 635-ter, 635-quater, 635-quinquies c.p.);** **Art. 25-septies d.lgs 231/2001;** **Art. 25-novies d.lgs 231/2001 (artt. 171, 171-bis, 171-ter, 174-sexies L. n. 633/1941)** **RISCHIO STRUMENTALE:** **tutti i rischi ritenuti rilevanti**

Incarichi di collaborazione e consulenza a persone fisiche	AD/ufficio interessato, Risorse Umane (Capogruppo) /Referente contratto di servizio/Personale interessato	Corruzione attiva e passiva; corruzione in atti giudiziari; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione tra privati, istigazione alla corruzione tra privati; intermediazione illecita e sfruttamento del lavoro; ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita; autoriciclaggio; induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria; condotte favorenti l'immigrazione clandestina; impiego di cittadini di paesi terzi il cui soggiorno è irregolare; concussione; omicidio colposo e lesioni gravi o gravissime colpose - commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro	**RISCHIO DIRETTO:** **Art. 25 d.lgs. 231/2001 (artt. 318, 319, 319 ter, 319 quater; 320, 321, 322, 346 bis cp);** **Art. 25-ter (artt. 2635, 2635 bis cc);** **Art. 25-quinquies (art. 603 bis cp);** **Art. 25-octies d.lgs 231/2001;** **Art. 25-decies d.lgs 231/2001 (art. 377 bis c.p.);** **Art. 25-duodecies (artt. 12, commi 3, 3-bis, 3-ter e 5, e art. 22, comma 12-bis, d. lgs n. 286/1998)** **RISCHIO STRUMENTALE:** **Art. 25 d.lgs 231/2001 (artt. 317; 318, 319, 319-quater c.p.);** **Art. 25-septies d.lgs 231/2001**
Gestione presenze e trasferte	AD/ufficio interessato, Risorse Umane (Capogruppo)/ Referente contratto di servizio	Malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; Corruzione attiva e passiva; corruzione in atti giudiziari; induzione indebita a dare o promettere utilità; istigazione alla corruzione; induzione indebita a dare o promettere utilità, corruzione attiva e passiva, corruzione in atti giudiziari, istigazione alla corruzione - di membri degli organi UE o di funzionari UE; ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita; autoriciclaggio	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (316-bis, 316-ter, 640, 640-bis, 640-ter c.p.);** **ART. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316 c.p.)** **RISCHIO STRUMENTALE:** **Art. 25 d.lgs 231/2001 (artt. 318, 319, 319-ter, 319-quater, 320, 321, 322, 322-bis c.p.);** **Art. 25-octies d.lgs 231/2001**
Gestione informazioni riservate	AD/ufficio interessato, Risorse Umane (Capogruppo) /Referente contratto di servizio/Personale interessato	Falsità in documento pubblico informatico; accesso abusivo a sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; danneggiamento di sistemi informatici o telematici di pubblico interesse; Malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; accesso abusivo ad un sistema informatico o telematico; corruzione attiva e passiva, induzione indebita a dare o promettere utilità, istigazione alla corruzione; corruzione tra privati; istigazione alla corruzione tra privati; abuso o comunicazione illecita di informazioni privilegiate - raccomandazione o induzione di altri alla commissione di abuso di informazioni privilegiate; ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita; autoriciclaggio; condotte favorenti l'immigrazione clandestina; Impiego di cittadini di paesi terzi il cui soggiorno è irregolare	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter, 635-quinquies c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 640, 640-bis c.p.);** **Art. 24-bis d.lgs 231/2001 (art. 615-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 318, 319, 319-quater, 320, 321, 322 c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis c.c.);** **Art. 25-sexies (art. 184 TUF);** **Art. 25-octies d.lgs 231/2001;** **Art. 25-duodecies (artt. 12, commi 3, 3-bis, 3-ter e 5, e art. 22, comma 12-bis, d.lgs. 286/1998)**

IV.8.2. ELEMENTI DI CONTROLLO RISORSE UMANE

Per le attività relative alla selezione, assunzione e sviluppo delle risorse umane, il Responsabile di processo coincide con la Funzione competente di Capogruppo, con l'Amministratore Delegato e con i Referenti interni a Infratel Italia per la gestione degli aspetti relativi alle Risorse Umane.
L'Amministratore Delegato e i Referenti interni coinvolti garantiscono il rispetto delle attività espletate dalla Capogruppo.

IV.8.2.1. Selezione e assunzione del personale

Infratel Italia, avvalendosi della Funzione Risorse Umane della Capogruppo, in accordo alle policy di Capogruppo, assicura che il processo di ricerca e selezione del personale[56] sia condotto nel rispetto delle normative vigenti - nazionali e comunitarie in materia di reclutamento del personale delle società pubbliche e sulla base dei seguenti principi:

- valorizzazione delle risorse interne e ottimizzazione dell'organizzazione- per qualsiasi fabbisogno viene operata la ricerca di personale, già impiegato nel Gruppo, prima di attivare la ricerca sul mercato esterno;
- pubblicità e trasparenza - ogni ricerca esterna di personale viene tempestivamente pubblicata sul sito esterno della Capogruppo;
- oggettività - la valutazione delle candidature viene effettuata sulla base di requisiti, essenziali e non discriminatori, necessari per la copertura delle posizioni vacanti, definiti precedentemente all'avvio della ricerca;
- imparzialità - per l'individuazione della risorsa si provvede alla predisposizione di una graduatoria dei candidati idonei individuati in funzione della loro idoneità professionali, valutata sulla base dei requisiti essenziali per lo svolgimento della prestazione richiesta e non discriminatori;
- le candidature sono valutate attraverso un processo di selezione predeterminato e diversamente articolato in funzione delle caratteristiche della posizione e del livello di esperienza richiesto (colloqui di gruppo, test, colloqui individuali anche eseguiti da società esterne indipendenti).

L'Amministratore Delegato, in collaborazione con la Funzione Risorse Umane presso la Capogruppo e con le funzioni aziendali interessate, assicura il processo periodico di pianificazione dell'organico della Società.

Il processo di ricerca e selezione del personale, nel rispetto delle normative nazionali ed euro-unitarie applicabili, avviene:

- attraverso il confronto di più soggetti candidati idonei rispetto ai requisiti richiesti;
- attraverso il coinvolgimento della funzione richiedente di Infratel Italia, di risorse competenti della Capogruppo e di terze parti indipendenti - queste ultime laddove previsto dalla normativa vigente - nella fase di ricerca, valutazione e selezione dei candidati;
- sulla base di una valutazione condivisa delle capacità tecnico-professionali e attitudinali delle risorse esaminate.

Le proposte economico contrattuali sono in linea con le policies di gruppo e/o i CCNL di riferimento, ovvero i valori di mercato in relazione alla tipologia di consulenza/collaborazione e alla figura professionale interessata, quindi autorizzate dall'Amministratore Delegato.

Sono accertati e valutati, anche mediante autocertificazione, nel corso dell'iter di selezione, i rapporti, diretti o indiretti, di ciascun candidato con soggetti della Pubblica Amministrazione o facenti capo ai fornitori/partner della Società.

Deve essere effettuata una verifica di affidabilità/onorabilità del candidato prescelto attraverso l'acquisizione di un'autodichiarazione, ai sensi della normativa vigente, circa il possesso dei suddetti requisiti.

In aggiunta, nell'impiego di collaboratori esterni è assicurata:

- la presenza, nei contratti di collaborazione, di opportune clausole di risoluzione in caso di inosservanza o violazione del Codice Etico, delle disposizioni del Modello 231, Parte Generale e Parte Speciale, e del Piano di Prevenzione della Corruzione ai sensi della L.190/2012 nonché di eventuali regole operative imposte nell'espletamento della prestazione. Deve essere assicurata la ricezione e presa visione da parte del

[56] Anche collaboratori/consulenti

collaboratore dei suddetti documenti anche attraverso la consegna della copia controfirmata;

- la presenza, nei contratti di collaborazione/consulenza, di opportune clausole di risoluzione in caso di violazione degli obblighi di riservatezza nel trattamento delle informazioni aziendali;
- l'applicazione di opportuni meccanismi di verifica, anche mediante autodichiarazione del collaboratore esterno, circa l'insussistenza di collaborazione sulla stessa materia con le corrispondenti amministrazioni pubbliche ai sensi della normativa vigente in materia di anticorruzione;
- la richiesta del conto corrente;
- l'effettiva erogazione della prestazione sulla base di quanto formalmente certificato dalla funzione richiedente in accordo agli obiettivi di progetto e/o della consulenza oggetto di incarico;
- l'applicazione di opportune policies di rotazione laddove possibile; qualora, per esigenze operative anche di continuità di azione da parte del collaboratore, fosse necessario ricorrere a incarichi ripetuti, la funzione richiedente deve motivare in forma scritta le suddette necessità;
- nei casi in cui sia prevista l'emissione della fattura da parte dell'incaricato, la verifica che la fattura corrisponda al contratto, quindi l'attivazione della Funzione Amministrazione presso la Capogruppo per l'erogazione del compenso, previa firma del mandato di pagamento da parte dei Soggetti interni titolati della Società.

I documenti/lettere/atti formali preordinati l'assunzione e/o la collaborazione devono essere firmati dall'Amministratore Delegato nonché dalla risorsa interessata.

In fase di inserimento di una nuova risorsa, è assicurata la consegna e la verifica di presa visione da parte della stessa, del Modello 231, Parte Generale e Parte Speciale, e del Piano di Prevenzione della Corruzione, tra cui l'informativa relativa alla privacy, alla tutela della riservatezza delle informazioni aziendali e sui rischi in materia di sicurezza sul lavoro specifici della mansione da ricoprire.

La Funzione Risorse Umane presso la Capogruppo assicura il rispetto degli adempimenti di legge inerenti le autorizzazioni per le assunzioni agevolate garantendo, nella predisposizione della relativa documentazione, diligenza e professionalità al fine di fornire agli enti pubblici competenti informazioni chiare, complete e veritiere.

La Funzione Risorse Umane presso la Capogruppo provvede altresì a un'attività periodica di monitoraggio, in coordinamento con la funzione Amministrazione, della giacenza/movimentazione dei buoni pasto dedicati al personale.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate, la Funzione Risorse Umane presso la Capogruppo, anche per il tramite delle funzioni competenti interne, è tenuta alla comunicazione periodica, su base annuale, all'Amministratore delegato, all'OdV ed al RPCT di un'informazione riepilogativa di tutte le assunzioni/inserimenti effettuati nel periodo, con indicazione della funzione di destinazione, del tipo di iter seguito, della tipologia di contratto, anche specificando gli eventuali rapporti accertati con la Pubblica Amministrazione o fornitori/partner commerciali della Società, delle proroghe o trasformazioni effettuate nel periodo, delle integrazioni ai contratti di collaborazione in essere, delle richieste autorizzate di retribuzioni non in linea con le policy aziendali e CCNL, e di una tempestiva comunicazione all'Amministratore delegato, al Responsabile della Trasparenza ed al Responsabile del Sistema di Gestione Salute e Sicurezza sul Lavoro, di tutte le singole nuove assunzioni/inserimenti/cessazioni, al fine di adempiere agli obblighi relativi alle normative in materia di "trasparenza" e "sicurezza sui luoghi di lavoro".

In ogni caso, il responsabile della Funzione Risorse Umane presso la Capogruppo comunica all'OdV e al RPCT, con cadenza almeno annuale, le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

IV.8.2.2. Impiego di personale di paesi non appartenenti all'Unione Europea

In aggiunta ai protocolli di gestione definiti per il processo di selezione e assunzione del personale, l'Amministratore delegato di Infratel Italia, in coordinamento con la Funzione Risorse Umane presso la Capogruppo e in accordo alle policies di Capogruppo, assicura che il processo di assunzione e/o impiego di cittadini di Paesi Terzi avvenga nel rispetto della normativa vigente in materia di immigrazione. In particolare, la Funzione Risorse Umane presso la Capogruppo si occupa delle seguenti incombenze:

- deve essere formalizzata, in fase di selezione, la motivazione relativa alla decisione di consentire/richiedere l'ingresso di una persona nel territorio italiano;
- deve essere garantita la corretta attuazione delle procedure operative per l'assunzione di personale estero definite dagli organi competenti (es. Ministero degli Interni, Uffici Immigrazione);
- deve essere verificato l'ingresso in Italia del lavoratore straniero in coerenza con le motivazioni addotte;
- deve essere effettuato il controllo di validità del permesso di soggiorno e/o si deve provvedere alla preventiva stipulazione del contratto di soggiorno qualora il lavoratore straniero sia già soggiornante in Italia;
- deve essere assicurato il mantenimento dei requisiti di validità del permesso di soggiorno (scadenza, richiesta di rinnovo, rinnovo o revoca), attivando le opportune azioni, anche coinvolgendo la Funzione Legale presso la Capogruppo qualora dovessero essere riscontrate o potrebbero riscontrarsi violazioni dei suddetti requisiti e comunicando tempestivamente l'anomalia all'Organismo di Vigilanza.

Qualora ci si avvalga di eventuali soggetti terzi, che operano in nome e per conto della Società, per l'effettuazione delle suddette attività, questi dovranno garantire, attraverso la propria struttura organizzativa, il recepimento degli elementi di controllo definiti.

La Funzione Risorse Umane presso la Capogruppo assicura che il processo di assunzione e/o impiego di cittadini di Paesi Terzi avvenga nel rispetto della normativa vigente in materia di immigrazione e comunica all'Organismo di Vigilanza, anche coinvolgendo il la Funzione Legale presso la Capogruppo, eventuali anomalie relative alla violazione dei requisiti di legge.

IV.8.2.3. Sviluppo e incentivazione delle risorse

Infratel Italia assicura trasparenza ed imparzialità nel processo di valutazione e crescita professionale delle proprie risorse a tutti i livelli; i sistemi di sviluppo delle carriere e di incentivazione di volta in volta adottati sono oggettivi e commisurati alle performance individuali ed aziendali.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate, Risorse Umane presso la Capogruppo è tenuta alla comunicazione periodica, su base annuale, all'Amministratore delegato, all'Organismo di Vigilanza, al RPCT ed al Responsabile Trasparenza di un'informativa riepilogativa degli incentivi/aumenti di categoria/premi di produzione assegnati e del sistema degli obiettivi definiti e del grado di raggiungimento.

In ogni caso, il responsabile della Funzione Risorse Umane presso la Capogruppo comunica all'OdV e al RPCT, con cadenza almeno annuale, le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

IV.8.2.4. Formazione

Infratel Italia assicura, nell'ambito del processo di formazione del personale, il rispetto della normativa applicabile in materia di diritto d'autore.

In particolare, Risorse Umane presso la Capogruppo sovraintende e garantisce:

- la diffusione di codici di condotta da utilizzarsi per la preparazione del materiale didattico, atti a vietare la duplicazione oltre i limiti di legge e la distribuzione di testi protetti dal diritto di autore;
- la citazione degli autori del materiale che viene distribuito;
- qualora fosse necessario fotocopiare, scansionare, includere in una piattaforma e-learning materiali didattici protetti dal diritto di autore, la richiesta e l'ottenimento di un esplicito permesso dell'autore o altro soggetto titolato;
- anche in collaborazione con la Funzione Legale della Capogruppo, la presenza nei contratti stipulati con società/docenti esterni di specifiche clausole inerenti il diritto d'autore quali, a titolo indicativo:
  - autorizzazione, da parte del docente, a distribuire i materiali prodotti ai discenti o più in generale ai dipendenti qualora si voglia utilizzare il materiale didattico anche in un secondo momento;
  - obbligo da parte del docente di utilizzare solamente materiali originali o comunque che abbia il diritto di autorizzare Infratel Italia alla riproduzione;
  - autorizzazione, da parte del docente, a modificare i testi didattici.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate, la Funzione Risorse Umane presso la Capogruppo è tenuta alla comunicazione periodica, su base annuale, all'Amministratore delegato e all'Organismo di Vigilanza di un'informativa riepilogativa delle eventuali sessioni formative organizzate, riportante il dettaglio dei partecipanti e degli argomenti trattati.

In ogni caso, il responsabile della Funzione Risorse Umane presso la Capogruppo comunica all'OdV e al RPCT, con cadenza almeno annuale, le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

IV.9 SUPPORTO OPERATIVO PIATTAFORMA DI GARA

Sono affidate alla Capogruppo le attività relative all'implementazione di strumenti di comunicazione digitale (es. firma digitale e PEC) tali da aumentare l'efficienza degli iter di gara telematica sul portale personalizzato.

IV.9.1. ATTIVITÀ A RISCHIO E POTENZIALI REATI (SUPPORTO OPERATIVO PIATTAFORMA DI GARA)

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Supporto all'ufficio pianificazione e gare per la cura dei procedimenti di affidamento, per il rispetto di adempimenti normativi e del sistema di e-procurement	Service Capogruppo, RUP, PGI, Gare e assistenza RUP	Malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; truffa in danno dello Stato o altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; frode nelle pubbliche forniture; turbata libertà degli incanti; turbata libertà del procedimento di scelta del contraente; falsità in documento pubblico informatico; accesso abusivo a sistema informatico o telematico; detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici; intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche; detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche; detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche; danneggiamento di informazioni, dati e programmi informatici, anche utilizzati dallo Stato o altro ente pubblico o comunque di pubblica utilità; danneggiamento di sistemi informatici o telematici; detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico; danneggiamento di sistemi informatici o telematici di pubblico interesse; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; concussione; corruzione attiva o passiva; corruzione in atti giudiziari; induzione indebita a dare o promettere utilità; istigazione alla corruzione; induzione indebita a dare o promettere utilità, corruzione attiva e passiva, corruzione in atti giudiziari e istigazione alla corruzione - di membri degli organi UE o di funzionari UE; traffico di influenze illecite; corruzione tra privati; istigazione alla corruzione tra privati; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza;	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 640, 640-bis, 640-ter, 356, 353, 353-bis c.p.);** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 615-quater, 617-quater, 617.quinquies, 635-bis, 635-ter, 635-quater, 635-quater.1, 635-quinquies c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 317, 318, 319, 319-ter, 320, 321, 322, 322-bis, 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis, 2638 c.c.)**

IV.9.2. ELEMENTI DI CONTROLLO PIATTAFORMA DI GARA

Per le attività relative al supporto operativo della piattaforma di gara e della gestione dell'Albo fornitori della Capogruppo, il Responsabile di processo coincide con la Funzione competente di Capogruppo, con l'Amministratore Delegato e con i Referenti interni a Infratel Italia per la gestione degli aspetti relativi alla Pianificazione e Gestione Gare.
L'Amministratore Delegato e i Referenti interni coinvolti garantiscono il rispetto delle attività espletate dalla Capogruppo.

IV.10 CURA DEI PROCEDIMENTI DI AFFIDAMENTO PER IL RISPETTO DI ADEMPIMENTI NORMATIVI E DEL SISTEMA DI E-PROCUREMENT E GESTIONE DELL'ALBO FORNITORI DELLA CAPOGRUPPO

Per i controlli specifici applicabili a tale attività si rinvia al paragrafo relativo nell'ambito dell'unità **Pianificazione Gare e Ingegneria**, e dell'unità **Acquisti, Affari Generali e Demand Organizzazione,** con specifico riferimento alla cura dei procedimenti di affidamento per il rispetto di adempimenti normativi e del sistema di e-procurement che include la gestione dell'Albo fornitori della Capogruppo.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate all'Organismo di Vigilanza, la Funzione Supporto Operativo Piattaforme di Gara è tenuto alla comunicazione periodica, su base semestrale, di un'informativa riepilogativa di tutte le gare indette, specificando per ognuna di esse la natura del supporto fornito al competente Ufficio di Infratel Italia, i soggetti intervenuti e gli strumenti informativi utilizzati.

In ogni caso, il responsabile dell'Ufficio Supporto Operativo Piattaforme di Gara presso la Capogruppo comunica all'OdV e al RPCT, con cadenza almeno annuale, le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

CAPITOLO V MISURE SPECIFICHE PER I PROCESSI DI BUSINESS E DI SUPPORTO OPERATIVO

V.1 AREE A RIPORTO DEL DIRETTORE GENERALE

L'attività a riporto del Direttore Generale è organizzata essenzialmente in quattro rami operativi.
I due principali, affidati alle figure dirigenziali munite di procura del D.G. stesso, curano i principali piani di *business* della Società (Infrastrutture e Operations e Reti Mobili e Connettività).
Inoltre, riportano direttamente al Direttore Generale l'unità Piano 5G Densificazione, che cura in autonomia le attività legate al relativo piano e l'unità Rendicontazione, unità di supporto di importanza trasversale, per l'attività delle verifiche economiche, che si accompagnano a quelle tecniche svolte dalle unità *business*.
A sua volta, l'unità rendicontazione è frazionata in due sottounità, cui è affidata la verifica economica delle attività finanziate. Le unità di secondo livello sono specializzate per circuito finanziario e amministrazione di riferimento (rispettivamente, MIMIT e DTD), in ragione dei differenti principi contabili e organizzativi applicati nelle rispettive attività di controllo.

L'attività di *risk assessment* delle aree *business* ha affrontato analiticamente ciascuna unità, di cui vi è evidenza nelle tabelle di valutazione. Gli elementi di controllo sono affrontati congiuntamente per i processi di Rendicontazione e individualmente per il Piano 5G Densificazione.
Per quanto attiene l'area business "Reti Mobili e Connettività", gli elementi di controllo sono stati indicati congiuntamente per i piani Voucher, Sanità Connessa, Wifi e Servizi Digitali, Piano Italia 5G, Scuole Connesse.
Per quanto attiene l'area *business* "Infrastrutture e Operations", invece, sono previste specifiche misure di mitigazione per Gestione Rete, Gestione SINFI, Business Development, mentre sono accorpati gli elementi di controllo relativi alle singole "Aree Operations", in ragione del fatto che le attività sono le medesime per tutte le aree (trattandosi di mera distribuzione territoriale), ad eccezione del "Piano Isole Minori", che interessa solo l'Area Operations "Isole", a cui è dedicato un paragrafo specifico.

V.2 RENDICONTAZIONE

L'unità si occupa del processo di rendicontazione delle attività svolte da beneficiari privati, concessionari, affidatari e dalla Società, per le attività ed i servizi resi in favore del Committente pubblico o privato.

V.2.1. ATTIVITÀ A RISCHIO E POTENZIALI REATI (RENDICONTAZIONE E CIRCUITO FINANZIARIO DTD)

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Controllo dei consuntivi delle spese effettivamente sostenute per l'attuazione delle attività dei progetti aziendali sulla base delle convenzioni sottoscritte	Responsabile di funzione	Malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; falsità in documento pubblico informatico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 356, 640, 640-bis, 640-ter c.p.);** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 635-bis, 635-ter);** **Art. 25 d.lgs 231/2001 (artt. 317, 318, 319, 319-quater, 320, 321, 322, 346-bis, c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 356, 640, 640-bis, 640-ter c.p.);**

		- quando i fatti offendono gli interessi finanziari dell'UE; impedito controllo; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita; autoriciclaggio; dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti; dichiarazione fraudolenta mediante altri artifici; dichiarazione infedele; emissione di fatture o altri documenti per operazioni inesistenti; occultamento o distruzione di documenti contabili; indebita compensazione; sottrazione fraudolenta al pagamento di imposte	**Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316 c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2625, 2638 c.c.);** **Art. 25-octies d.lgs 231/2001;** **Art. 25-quinquiesdecies d.lgs 231/2001 (artt. 2, 3, 4, 8, 10, 10-quater, 11 d.lgs 74/2000)**
Coordinamento, gestione e monitoraggio del processo di rendicontazione (DTD)	Responsabile di funzione, D.G., A.D.	Malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; falsità in documento pubblico informatico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; impedito controllo; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita; autoriciclaggio; dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti; dichiarazione fraudolenta mediante altri artifici; dichiarazione infedele; emissione di fatture o altri documenti per operazioni inesistenti; occultamento o distruzione di documenti contabili; indebita compensazione; sottrazione fraudolenta al pagamento di imposte	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 356, 640, 640-bis, 640-ter c.p.);** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 635-bis, 635-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 317, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 356, 640, 640-bis, 640-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316 c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2625, 2638 c.c.);** **Art. 25-octies d.lgs 231/2001** **Art. 25-quinquiesdecies d.lgs 231/2001 (artt. 2, 3, 4, 8, 10, 10-quater, 11 d.lgs. 74/2000)**
Supporto all'unità organizzativa Controllo di Gestione (DTD)	Responsabile di funzione	Corruzione tra privati; istigazione alla corruzione tra privati; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite	**RISCHIO DIRETTO:** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis, 2638 c.c.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 640, 640-bis, 640-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 318, 319, 319-quater, 320, 321, 322, 346-bis, c.p.)**

Verifica delle spese degli operatori (DTD)	Responsabile di funzione, D.G.	Malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; falsità in documento pubblico informatico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione tra privati; istigazione alla corruzione tra privati; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 356, 640, 640-bis, 640-ter c.p.);** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 635-bis, 635-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 317, 318, 319, 319-quater, 320, 321, 322, 346-bis, c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis, 2638 c.c.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 640, 640-bis, 640-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 317, 318, 319, 319-quater, 320, 321, 322, 346-bis, c.p.)**
Monitoraggio stato avanzamento dei target previsti dai Piani Operativi Finanziati (DTD)	Responsabile di funzione, D.G., A.D.	Falsità in documento pubblico informatico; accesso abusivo ad un sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; indebita destinazione di denaro o cose mobili quando offende gli interessi finanziari dell'UE; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione tra privati; istigazione alla corruzione tra privati; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; peculato, peculato mediante profitto dell'errore altrui - quando i fatti offendono gli interessi finanziari dell'UE; induzione indebita a dare o promettere utilità, corruzione attiva e passiva, corruzione in atti giudiziari, istigazione alla corruzione - di membri degli organi UE o di funzionari UE	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.);** **Art. 25 d-lgs 231/2001 (artt. 314-bis, 317, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis, 2638 cod. civ.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 640, 640-bis, 640-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 317, 318, 319, 319-quater, 320, 321, 322, 322-bis, 346-bis c.p.)**
Implementazione sistema informatico di dialogo tramite la Piattaforma REGIS (sistema di monitoraggio e rendicontazione progetti PNRR) - (DTD)	Responsabile di funzione	Falsità in documento pubblico informatico; accesso abusivo ad un sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; , corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; induzione indebita a dare o promettere utilità, corruzione attiva e passiva, corruzione in atti giudiziari, istigazione alla corruzione - di membri degli organi UE o di funzionari UE; traffico di influenze illecite	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 640, 640-bis, 640-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 318, 319, 319-quater, 320, 321, 322, 322-bis, 346-bis c.p.)**
Gestione del circuito finanziario del ciclo di vita dei fondi (DTD)	Responsabile di funzione, D.G., A.D.	Malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; concussione; corruzione attiva o passiva; corruzione in atti giudiziari; induzione indebita a dare o promettere utilità; istigazione alla corruzione; induzione indebita a dare o promettere utilità, corruzione attiva e passiva, corruzione in atti	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 640, 640-bis, 640-ter c.p.);** **Art. 25 d.lgs 231/2001**

		giudiziari e istigazione alla corruzione di membri degli organi UE o di funzionari UE; traffico di influenze illecite	

V.2.2. ATTIVITÀ A RISCHIO E POTENZIALI REATI (RENDICONTAZIONE MIMIT)

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Gestione del processo di rendicontazione delle attività in convenzione (MIMIT)	Responsabile di funzione, D.G., A.D.	Falsità in documento pubblico informatico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; impedito controllo; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita; autoriciclaggio; dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti; dichiarazione fraudolenta mediante altri artifici; dichiarazione infedele; emissione di fatture o altri documenti per operazioni inesistenti; occultamento o distruzione di documenti contabili; indebita compensazione; sottrazione fraudolenta al pagamento di imposte	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 635-bis, 635-ter);** **Art. 25 d.lgs 231/2001 (artt. 317, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 356, 640, 640-bis, 640-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316 c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2625, 2638 c.c.);** **Art. 25-octies d.lgs 231/2001;** **Art. 25-quinquiesdecies d.lgs 231/2001 (artt. 2, 3, 4, 8, 10, 10-quater, 11 d.lgs. 74/2000)**
Definizione del sistema dei controlli sul beneficiario privato, monitoraggio dei beneficiari e verifiche di clawback (MIMIT)	Responsabile di funzione, D.G., A.D.	Falsità in documento pubblico informatico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; impedito controllo; corruzione tra privati, istigazione alla corruzione tra privati; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita; autoriciclaggio; dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti; dichiarazione fraudolenta mediante altri artifici; dichiarazione infedele; emissione di fatture o altri documenti per operazioni inesistenti; occultamento o distruzione di documenti contabili; indebita compensazione; sottrazione fraudolenta al pagamento di imposte	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 635-bis, 635-ter);** **Art. 25 d.lgs 231/2001 (artt. 317, 318, 319, 319-quater, 320, 321, 322, 346-bis, c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 356, 640, 640-bis, 640-ter c.p.);** **Art. 25 d.lgs 231/2001 (art.314, 314-bis, 316 c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2625, 2635, 2635-bis, 2638 c.c.);** **Art. 25-octies d.lgs 231/2001;** **Art. 25-quinquiesdecies d.lgs 231/2001 (artt. 2, 3, 4, 8, 10, 10-quater, 11 d.lgs. 74/2000)**

Raccolta, controllo e invio della documentazione di monitoraggio e rendicontazione ai competenti organi della Pubblica Amministrazione (MIMIT)	Responsabile di funzione, D.G., A.D.	Falsità in documento pubblico informatico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; impedito controllo; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; impedito controllo; corruzione tra privati, istigazione alla corruzione tra privati; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita; autoriciclaggio; dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti; dichiarazione fraudolenta mediante altri artifici; dichiarazione infedele; emissione di fatture o altri documenti per operazioni inesistenti; occultamento o distruzione di documenti contabili; indebita compensazione; sottrazione fraudolenta al pagamento di imposte	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 635-bis, 635-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 317, 318, 319, 319-quater, 320, 321, 322, 346-bis, c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2625, 2638 c.c.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 356, 640, 640-bis, 640-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316 c.p.);** **Art. 25-octies d.lgs 231/2001;** **Art. 25-quinquiesdecies d.lgs 231/2001 (artt. 2, 3, 4, 8, 10, 10-quater, 11 d.lgs. 74/2000)**
Monitoraggio e rendicontazione degli interventi di infrastrutturazione (MIMIT)	Responsabile di funzione, D.G., A.D.	Falsità in documento pubblico informatico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; impedito controllo; corruzione tra privati, istigazione alla corruzione tra privati; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; impedito controllo; corruzione tra privati, istigazione alla corruzione tra privati; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita; autoriciclaggio; dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti; dichiarazione fraudolenta mediante altri artifici; dichiarazione infedele; emissione di fatture o altri documenti per operazioni inesistenti; occultamento o distruzione di documenti contabili; indebita compensazione; sottrazione fraudolenta al pagamento di imposte	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 635-bis, 635-ter);** **Art. 25 d.lgs 231/2001 (artt. 317, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 356, 640, 640-bis, 640-ter, c.p.);** **Art. 25 d.lgs 231/2001 (art. 314, 314-bis, 316 c.p.);** **Art. 25-octies d.lgs 231/2001;** **Art. 25-quinquiesdecies d.lgs 231/2001 (artt. 2, 3, 4, 8, 10, 10-quater, 11 d.lgs. 74/2000)**

V.2.3. ELEMENTI DI CONTROLLO RENDICONTAZIONE

Per il complesso delle attività svolte dall'unità Rendicontazione Infratel Italia garantisce che tutte le attività di rendicontazione all'organismo nazionale e/o euro-unitario connesse alla destinazione dei finanziamenti/contributi/fondi nell'ambito dei programmi, contratti e convenzioni, contengano elementi veritieri e coerenti. A tal fine tutta l'**attività di rendicontazione prodotta da Infratel Italia deve essere archiviata in un apposito fascicolo**.

V.2.3.1. Gestione della rendicontazione. Disciplinare e rapporto di rendicontazione.

L'Ufficio Rendicontazione assicura prima dell'avvio del processo di rendicontazione, la corretta interpretazione del Disciplinare di rendicontazione allegato a ciascuna Convenzione; l'esito di tale attività può richiedere la predisposizione di un documento interno di linee guida operative nel caso in cui il Disciplinare di rendicontazione non riporti le modalità di rendicontazione anche in termini di costi/spese ammissibili, modalità di calcolo e documentazione da allegare ai Report di rendicontazione oggetto di comunicazione al committente;

Tale documento interno è formalmente comunicato da Rendicontazione alle funzioni aziendali interessate.

La predisposizione della documentazione da inviare al committente deve essere effettuata con la massima diligenza e professionalità in modo da fornire informazioni chiare, accurate, complete, fedeli e veritiere evitando e comunque segnalando eventuali situazioni di conflitto di interesse.

La **corretta consuntivazione delle attività e dei costi effettivamente rendicontabili viene effettuata dall'unità Rendicontazione** sulla base delle informazioni ricevute dalle funzioni competenti e dai soggetti responsabili dell'esecuzione e monitoraggio delle commesse/interventi, secondo quanto stabilito dai Disciplinari di riferimento. In particolare, i soggetti interni preposti svolgono opportune attività di monitoraggio e verifica di assenza di conflitto di interesse, in relazione ad eventuali soggetti terzi coinvolti nella gestione delle commesse/interventi.
L'attività rendicontativa si basa sull'utilizzo di **sistemi applicativi dedicati**, attraverso i quali è tenuta traccia delle attività effettivamente svolte nell'ambito delle commesse/progetti, atti a garantire l'**utilizzo degli applicativi ai soli utenti autorizzati**, la **tracciabilità di tutte le operazioni di inserimento**, modifica e cancellazione e l'accessibilità delle informazioni contenute, provenienti da comunicazioni formali (report di monitoraggio) effettuate dalle funzioni aziendali competenti e/o coinvolte nel processo di esecuzione delle attività di commessa.

L'Ufficio Rendicontazione predispone il **rapporto di Rendicontazione** completo di tutta la documentazione giustificativa prevista dal contratto/convenzione, sulla base delle determinazioni di cui sopra e nel rispetto delle modalità definite nel Disciplinare applicabile, quindi verificato ed approvato dall'Amministratore Delegato e comunicato formalmente al committente dai Soggetti titolati della Società.
L'Ufficio Rendicontazione fornisce le informazioni alla funzione in service di Amministrazione per l'elaborazione, qualora prevista, della **fattura attiva associata al rapporto rendicontativo**; l'emissione della fattura da parte della funzione Amministrazione di Capogruppo viene quindi **comunicata formalmente al committente dai Soggetti titolati della Società**. Le attività che prevedono comunicazioni e/o incontri formali con soggetti rappresentanti del committente devono essere tracciate, fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate, l'Ufficio Rendicontazione è tenuto alla comunicazione periodica, su base annuale, all'Organismo di Vigilanza, al Direttore Generale e al RPCT, se di competenza, di un'informativa riepilogativa dell'attività svolta per tipologia di commessa/progetto e dei relativi importi rendicontati.

In ogni caso, il responsabile dell'Ufficio Rendicontazione comunica all'OdV e al RPCT, con cadenza almeno annuale, le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

V.2.3.2. Monitoraggio e implementazione sistema informatico di dialogo tramite la Piattaforma REGIS

La tracciabilità delle operazioni è strettamente correlata al coordinamento con l'unità Controllo di Gestione, per la trasmissione e il monitoraggio dei dati, anche attraverso l'implementazione di apposito canale informatico.

L'unità rendicontazione è referente per la raccolta, controllo e invio della documentazione di monitoraggio e rendicontazione ai competenti organi della Pubblica Amministrazione, per le attività di monitoraggio svolte dalla Capogruppo e dagli altri organismi di controllo esterni.
L'attività di inserimento dati di rendicontazione è svolta in osservanza dei principi generali di trasparenza, correttezza e tracciabilità. L'uso delle piattaforme operative e dei relativi *account* si conforma, oltre a quelle eventualmente predisposte dal *provider* esterno, alle specifiche misure di sicurezza previste nell'ambito del trattamento dati e sicurezza informatica, cui si rinvia.
Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate, l'Ufficio Rendicontazione è tenuto alla comunicazione periodica, su base annuale, all'Organismo di Vigilanza, al RPCT e al Direttore Generale di un'informativa riepilogativa dei dati raccolti per tipologia di commessa/progetto e dei relativi importi rendicontati.

In ogni caso, il responsabile dell'Ufficio Rendicontazione comunica all'OdV e al RPCT, con cadenza almeno annuale, le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

V.2.3.3. Ulteriori attività di supporto e di controllo affidate all'unità Rendicontazione.

Tra le responsabilità dell'unità organizzativa Rendicontazione vi è quella della definizione della struttura di accounting separation eventualmente necessaria ai processi di rendicontazione (Rendicontazione MIMIT).
Nella mappatura dei rischi tale attività risulta meramente strumentale, in quanto consiste in una verifica di conformità priva di un significativo margine di esposizione. . Tuttavia, non si può escludere che una grave carenza nel suo svolgimento possa agevolare od occultare la commissione di un illecito, né, altresì, può escludersi che i responsabili di tali funzioni partecipino in concorso con le funzioni coinvolte in altre ipotesi di rischio, divenendo in tal caso essi stessi direttamente autori dell'illecito.
Di seguito il riepilogo delle attività meramente strumentali:

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Definizione della struttura di accounting separation eventualmente necessaria ai processi di rendicontazione. (MIMIT)	Responsabile di funzione, D.G., A.D.	Falsità in documento informatico pubblico; Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.); Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità	**RISCHIO STRUMENTALE: Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 635-bis, 635-ter c.p.)**

Al fine di prevenire gli ulteriori rischi di illecito correlati a queste attività meramente strumentali, il *risk owner* di primo livello svolge la propria attività in coordinamento con le altre funzioni interne e della Capogruppo coinvolte, rispettando i principi generali di controllo e il codice etico, avendo come punti di attenzione i rischi strumentali sopra indicati.

Il process owner garantisce l'effettività e l'efficacia dei controlli, adeguando periodicamente le procedure. A tal fine richiede una informativa ai risk owner, sulla base della quale egli acquisisce le informazioni rilevanti per attuare le opportune azioni correttive e alimentare i flussi informativi, segnalando tempestivamente all'OdV, e al RPCT se di competenza, eventuali anomalie o non conformità riscontrate.

V.3 PIANO ITALIA 5G DENSIFICAZIONE

Sono affidate all'unità Piano Italia 5G densificazione le attività di attuazione del Piano Italia 5G.

V.3.1. ATTIVITÀ A RISCHIO E POTENZIALI REATI

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Definizione procedure operative, controlli e documentazione piano Italia 5G	Responsabile di funzione, D.G., A.D.	Truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; falsità in documento pubblico informatico; omicidio colposo e lesioni gravi o gravissime colpose - commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro; inquinamento ambientale; delitti colposi contro l'ambiente; distruzione o deterioramento di habitat all´interno di un sito protetto; indebita percezione di erogazioni pubbliche; accesso abusivo a sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; impedito controllo; corruzione tra privati; istigazione alla corruzione tra privati; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; inquinamento ambientale; delitti colposi contro l'ambiente; distruzione o deterioramento di habitat all'interno di un sito protetto	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (artt. 640, 640-bis, 640-ter c.p.);** **Art. 24-bis d.lgs 231/2001 (art. 491-bis c.p.);** **Art. 25-septies d.lgs 231/2001** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (art. 316-ter c.p.);** **Art. 24-bis d.lgs 231/2001 (artt. 615-ter, 635-bis, 635-ter c.p.);** **Art. 25 d.lgs 231/2001 (318, 319, 319-quater, 320, 321, 322 c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2625, 2635, 2635-bis, 2638 c.c.);** **Art. 25-undecies d.lgs 231/2001 (artt. 452-bis, 452-quinquies, 733-bis c.p.);**
Verifiche tecniche ed economiche piano Italia 5g	Team 5G, Responsabile di funzione	Falsità in documento pubblico informatico; accesso abusivo ad un sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione tra privati; istigazione alla corruzione tra privati; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; omicidio colposo e lesioni gravi o gravissime colpose - commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro; ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita; autoriciclaggio; inquinamento ambientale; delitti colposi contro l'ambiente; dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti; dichiarazione fraudolenta mediante altri artifici; emissione di fatture o altri documenti per operazioni inesistenti; occultamento o distruzione di documenti contabili	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 318, 319, 319-quater, 320, 322, 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis, 2638 c.c.);** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 356, 640, 640-bis, 640-ter c.p.);** **Art. 25-septies d.lgs 231/2001;** **Art. 25-octies d.lgs 231/2001;** **Art. 25-undecies (artt. 452-bis, 452-quinquies c.p.);** **Art. 25-quinquiesdecies d.lgs 231/2001 (artt. 2, 3, 8, 10 d.lgs 74/2000)**
Verifiche di copertura	Team 5G, Responsabile di funzione	Truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; falsità in documento pubblico informatico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione tra privati; istigazione alla corruzione tra privati; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; indebita percezione di erogazioni pubbliche;	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (artt. 640, 640-bis, 640-ter c.p.);** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 635-bis, 635-ter c.p.);** **Art. 25 d.lgs 231/2001 (318, 319, 319-quater, 320, 321, 322 c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis, 2638 c.c.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (art. 316-ter c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis, 2638 c.c.)**

Coordinamento DTD e gestione criticità con enti pubblici e privati	Responsabile di funzione, D.G., A.D.	Frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; falsità in documento pubblico informatico; accesso abusivo a sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; impedito controllo; corruzione tra privati; istigazione alla corruzione tra privati; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; inquinamento ambientale; delitti colposi contro l'ambiente; distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici; devastazione e saccheggio di beni culturali e paesaggistici	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (art. 640-ter);** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 317, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2625, 2635, 2635-bis, 2638 c.c.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 640, 640-bis c.p.);** **Art. 25-undecies (artt. 452-bis, 452-quinquies c.p.);** **Art. 25-septiesdecies (art. 518-duodecies c.p.);** **Art. 25-duodevicies (art. 518-terdecies c.p.)**

V.3.2. ELEMENTI DI CONTROLLO PIANO ITALIA 5G DENSIFICAZIONE

Per il complesso delle attività svolte dall'unità Piano Italia 5G Densificazione si rinvia alle regole di condotta previste per le aree Business Development e Reti Mobili e Connettività per i piani PNRR, per quanto di rilievo in merito alle modalità operative dei controlli tecnici ed economici e del recupero delle infrastrutture di rete, al fine di minimizzare l'impatto degli interventi da parte del beneficiario.

Tutti gli attori coinvolti hanno l'obbligo di comunicare tempestivamente all'Organismo di Vigilanza deroghe, anomalie o atipicità eventualmente riscontrate rispetto alle determinazioni stabilite per il presente processo.

Il responsabile dell'unità Piano 5G Densificazione è tenuto alla comunicazione periodica, su base annuale, all'Organismo di Vigilanza, al RPCT, al Direttore Generale e all'Amministratore Delegato di un'informativa sullo stato di avanzamento di ciascuna commessa/progetto e degli esiti delle verifiche/controlli effettuati.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate, l'unità 5G Densificazione, insieme all'Ufficio Controllo di Gestione, è tenuto alla comunicazione periodica, su base annuale all'OdV, al RPCT, al Direttore Generale e all'Amministratore Delegato di un'informativa riepilogativa del tempo effettivamente lavorato su ciascuna commessa/progetto aziendale da risorse interne.

In ogni caso, il responsabile dell'Ufficio 5G Densificazione comunica all'OdV e al RPCT, con cadenza almeno annuale, le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

V.4 RETI MOBILI E CONNETTIVITA'

L'unità organizzativa "Reti Mobili e Connettività" si occupa della realizzazione e gestione delle "commesse" (o progetti e piani) relative al servizio di connessione mobile e degli interventi infrastrutturali per i piani attuati direttamente, gestendo in particolare: le attività di accreditamento e controllo sui beneficiari privati; le verifiche tecniche ed esecutive per i lavori di realizzazione dei piani finanziati; la gestione e la manutenzione della rete wifi; la gestione e lo sviluppo degli altri servizi digitali.

V.4.1. ATTIVITÀ A RISCHIO E POTENZIALI REATI (RETI MOBILI E CONNETTIVITÀ)

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Funzione di RUP	Resp. funzione, Soggetti legittimati	Falsità in documento pubblico informatico; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione attiva o passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione e istigazione alla corruzione tra privati; omicidio o lesioni gravi e gravissime aggravati dalla violazione delle norme sulla prevenzione degli infortuni sul lavoro e delle malattie professionali; riciclaggio o rempiego in attività produttive di beni di provenineza illecita; rifiuto d'atti d'ufficio. omissione malversazione di beni pubblici; frode nelle pubbliche forniture; truffe, anche informatiche, ai danni di PA centrali o locali; inquinamento ambientale; disastro ambientale; delitti colposi contro l'ambiente; distruzione o deterioramento di habitat all'interno di un sito protetto; impiego di cittadini di paesi terzi irregolari; favoreggiamento della permanenza illegale dello straniero; dichiarazione ai fini delle imposte dirette o dell'IVA fraudolenta per uso di fatture false oggettivamente o soggettivamente, per altri artifici o altrimenti infedele; occultamento o distruzione dei documenti contabili; compensazione indebita ai danni dell'UE; sottrazione fraudolenta al pagamento di imposte; falsificazione in scrittura privata relativa a beni culturali; esportazione illecita di beni culturali; distruzione di beni culturali; riciclaggio di beni culturali	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (art. 491-bis c.p.);** **Art. 25 d.lgs. 231/2001 (artt. 314, 314-bis, 316, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25 ter d.lgs 231/2001 (art. 2635, 2635-bis c.c.);** **Art. 25-septies d.lgs 231/2001;** **Art. 25-octies d.lgs. 231/2001 (artt. 648-bis, 648-ter c.p.)** **L. 190/2012 (art. 328 c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 356, 640, 640-bis, 640-ter, c.p.);** **Art. 25-ter d.lgs 231/2001 (art. 2635, 2635-bis c.c.);** **Art. 25-undecies d.lgs 231/2001 (art. 452 bis, 452 quater, 452 quinquies, 733-bis c.p.);** **Art. 25-duodecies d.lgs 231/2001;** **Art. 25-quinquiesdecies d.lgs. 231/2001 (art. 2,3, 4, 5, 10, 10-quater, 11 d.lgs. 74/2000);** **Art. 25-septiesdecies d.lgs. 231/2001 (artt. 518-octies, 518-undecies; 518-duodecies c.p.);** **Art. 25-duodevicies d.lgs. 231/2001 (art. 518-sexies, c.p.)**

V.4.2. ATTIVITÀ A RISCHIO E POTENZIALI REATI (VOUCHER)

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Gestione operazioni di accreditamento degli operatori economici aderenti e validazione delle offerte commerciali	Responsabile di funzione	Accesso abusivo ad un sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione tra privati; malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; frode nell'esercizio del commercio	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (art. 615-ter, 635 bis, 635-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 317, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis c.c.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (art. 316-bis, 316-ter, 640, 640 bis, 640-ter c.p.);** **Art. 25-bis.1 d.lgs 231/2001 (art. 515 c.p.)**
ATTIVITÀ' SENSIBILI	**SOGGETTI**	**CONDOTTA ILLECITA**	**Fattispecie ex d.lgs. 231/2001**

Supporto al Ministero competente in relazione alle notifiche in sede comunitaria delle misure di aiuto con riferimento al Piano	Responsabile di funzione, A.D.	Falsità in documento pubblico informatico; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE	**RISCHIO DIRETTO:** **Art. 24 bis d.lgs 231/2001 (art. 491-bis cp);** **Art. 25-ter d.lgs 231/2001 (art. 2638 c.c.)** **RISCHIO STRUMENTALE** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 356, 640, 640-bis, 640-ter c.p.)**
Gestione delle richieste di prenotazione e attivazione dei voucher nonché pagamento agli operatori dei ratei di contributo maturati in relazione ai voucher attivati	Responsabile di funzione, Delegato, D.G., A.D.	Malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione tra privati; istigazione alla corruzione tra privati; accesso abusivo a sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita; autoriciclaggio	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 640, 640-bis, 640-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 317, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis c.c.)** **RISCHIO STRUMENTALE:** **Art. 24-bis d.lgs 231/2001 (artt. 615-ter, 635-bis, 635-ter c.p.);** **Art. 25-octies d.lgs 231/2001**
Controlli a campione in merito ai voucher prenotati o attivati	Responsabile di funzione, A.D.	Indebita percezione di erogazioni pubbliche; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; falsità in documento pubblico informatico; accesso abusivo ad un sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; malversazione di erogazioni pubbliche; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; corruzione tra privati; istigazione alla corruzione tra privati	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (artt. 316-ter, 640, 640 bis, 640-ter c.p.);** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 640, 640-bis c.p.);** **Art. 24-bis d.lgs 231/2001 (artt. 615-ter, 635-bis, 635-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 318, 319, 319-quater, 320, 321, 322 c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis c.c.)**

V.4.3. ULTERIORI ELEMENTI DI CONTROLLO PER PIANO VOUCHER

Tra le responsabilità dell'unità organizzativa *Piano Voucher* vi è quella del coordinamento delle attività di studio, ricerche e valutazioni di impatto con riferimento al Piano.
Nella mappatura dei rischi tale attività risulta meramente strumentale, in quanto consiste in attività di supporto, coordinamento e monitoraggio priva di un significativo margine di esposizione. Tuttavia, non si può escludere che una grave carenza del suo svolgimento possa agevolare od occultare la commissione di un illecito, né,

altresì, può escludersi che i responsabili di tale funzione partecipino in concorso con le funzioni coinvolte in altre ipotesi di rischio, divenendo in tal caso essi stessi direttamente autori dell'illecito.
Di seguito il riepilogo delle attività meramente strumentali:

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Coordinamento delle attività di studio, ricerche e valutazioni di impatto con riferimento al Piano	Responsabile di funzione	Indebita percezione di erogazioni pubbliche; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; corruzione attiva e passiva, induzione indebita a dare o promettere utilità, istigazione alla corruzione, traffico di influenze illecite; corruzione tra privati; istigazione alla corruzione tra privati	**RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 art. 316-ter, 640, 640 bis c.p.);** **Art. 25 d.lgs 231/2001 (artt. 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25 ter d.lgs 231/2001 (art. 2635, 2635-bis c.c.)**

Al fine di prevenire gli ulteriori rischi di illecito correlati a queste attività meramente strumentali, il *risk owner* di primo livello svolge la propria attività in coordinamento con le altre funzioni interne e della Capogruppo coinvolte, rispettando i principi generali di controllo e il codice etico, avendo come punti di attenzione i rischi strumentali sopra indicati.
Il process owner garantisce l'effettività e l'efficacia dei controlli, adeguando periodicamente le procedure. A tal fine richiede una informativa ai risk owner, sulla base della quale egli acquisisce le informazioni rilevanti per attuare le opportune azioni correttive e alimentare i flussi informativi, segnalando tempestivamente all'OdV, e al RPCT se di competenza, eventuali anomalie o non conformità riscontrate.

V.4.4. ATTIVITÀ A RISCHIO E POTENZIALI REATI (SANITÀ CONNESSA)

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Rapporti con i Gruppi di Lavoro Regionali per la raccolta degli elementi utili alla redazione dei Piani Tecnici Regionali	Resp. funzione	Falsità in documento pubblico informatico; accesso abusivo ad un sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE;	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 317, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 640, 640-bis, 640-ter c.p.)**
Redazione dei Piani Tecnici Regionali per la pianificazione e la progettazione degli interventi relative alle diverse strutture sanitarie	Resp. funzione	Falsità in documento pubblico informatico; malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; accesso abusivo ad un sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione tra privati; istigazione alla corruzione tra privati; inquinamento ambientale; delitti colposi contro l'ambiente	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (art. 491-bis c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 640, 640-bis, 640-ter c.p.);** **Art. 24-bis d.lgs 231/2001 (artt. 615-ter, 635-bis, 635-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 317, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (art. 2635, 2635-bis c.c.);** **Art. 25-undecies (artt. 452-bis, 452-quinquies c.p.)**

Approvazione dei progetti di connessione elaborati dagli Affidatari relativamente alle singole strutture sanitarie	Resp. funzione	Corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione tra privati; istigazione alla corruzione tra privati; malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; inquinamento ambientale; delitti colposi contro l'ambiente	**RISCHIO DIRETTO:** **Art. 25 d.lgs 231/2001 (artt. 318, 319, 320, 321, 322, 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis c.c.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 640, 640-bis, 640-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316 c.p.);** **Art. 25-undecies (artt. 452-bis, 452-quinquies c.p.)**
Verifica di conformità dei servizi e delle forniture contrattuali al fine di accertarne la regolare esecuzione	Resp. funzione	Falsità in documento pubblico informatico; accesso abusivo ad un sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione tra privati; istigazione alla corruzione tra privati; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita; autoriciclaggio; dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti; dichiarazione fraudolenta mediante altri artifici; emissione di fatture o altri documenti per operazioni inesistenti; occultamento o distruzione di documenti contabili	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 318, 319, 319-quater, 320, 322, 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis, 2638 c.c.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 356, 640, 640-bis, 640-ter c.p.);** **Art. 25-octies d.lgs 231/2001;** **Art. 25-quinquiesdecies d.lgs 231/2001 (artt. 2, 3, 8, 10 d.lgs 74/2000)**
Monitoraggio del rispetto degli SLA contrattuali relativi ai servizi attivati dalle strutture sanitarie	Resp. funzione	Frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; falsità in documento pubblico informatico; accesso abusivo ad un sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione tra privati; istigazione alla corruzione tra privati; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (art. 640-ter c.p.);** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 356, 640, 640-bis c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 318, 319, 319-quater, 320, 322 c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis, 2638 c.c.)**

Verifiche tecniche ed economiche sui lavori eseguiti attraverso il controllo della documentazione ed eventualmente attraverso controlli in situ su un campione di realizzazioni	Resp. funzione	Falsità in documento pubblico informatico; accesso abusivo ad un sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione tra privati; istigazione alla corruzione tra privati; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; omicidio colposo e lesioni gravi o gravissime colpose - commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro; ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita; autoriciclaggio; inquinamento ambientale; delitti colposi contro l'ambiente; dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti; dichiarazione fraudolenta mediante altri artifici; emissione di fatture o altri documenti per operazioni inesistenti; occultamento o distruzione di documenti contabili	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 318, 319, 319-quater, 320, 322, 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis, 2638 c.c.);** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 356, 640, 640-bis, 640-ter c.p.);** **Art. 25-septies d.lgs 231/2001;** **Art. 25-octies d.lgs 231/2001;** **Art. 25-undecies (artt. 452-bis, 452-quinquies c.p.);** **Art. 25-quinquiesdecies d.lgs 231/2001 (artt. 2, 3, 8, 10 d.lgs 74/2000)**
Coordinamento in collaborazione con il Dipartimento della Trasformazione Digitale, per le attività di monitoraggio delle milestone previste dal PNRR e per la divulgazione dei contenuti tecnici del Piano verso gli Enti e le Regioni.	Resp. funzione/Resp. RMC/D.G./A.D.	Falsità in documento pubblico informatico; accesso abusivo ad un sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; abuso o comunicazione illecita di informazioni privilegiate - raccomandazione o induzione di altri alla commissione di abuso di informazioni privilegiate	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 356, 640, 640-bis, 640-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (art. 2638 c.c.);** **Art. 25-sexies d.lgs 231/2001 (184 TUF)**

V.4.5. ATTIVITÀ A RISCHIO E POTENZIALI REATI (WIFI E SERVIZI DIGITALI)

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001

Pianificazione e sviluppo della rete WiFi in conformità ai Piani di Commessa del Progetto Piazza WiFItalia e di tutti i servizi digitali	Resp. funzione	Malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; falsità in documento pubblico informatico; accesso abusivo ad un sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione tra privati; istigazione alla corruzione tra privati; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; omicidio colposo e lesioni gravi o gravissime colpose - commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro; rifiuto d'atti d'ufficio. omissione ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita; autoriciclaggio; inquinamento ambientale; delitti colposi contro l'ambiente; distruzione o deterioramento di habitat all'interno di un sito protetto	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 356, 640, 640-bis, 640-ter c.p.);** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.);** **Art 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 317, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis, 2638 c.c.);** **Art. 25-septies d.lgs 231/2001** **L. 190/2012 (art. 328 c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (art. 316-ter);** **Art. 25-octies d.lgs 231/2001;** **Art. 25-undecies d.lgs 231/2001 (artt. 452-bis, 452-quinquies, 733-bis c.p.)**
Gestione e manutenzione della rete WiFi in conformità ai Piani di Commessa del Progetto talia e di tutti i servizi digitali	Resp. funzione	Malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; falsità in documento pubblico informatico; accesso abusivo ad un sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; omicidio colposo e lesioni gravi o gravissime colpose - commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro; ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita; autoriciclaggio; Peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione tra privati; istigazione alla corruzione tra privati; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; inquinamento ambientale; delitti colposi contro l'ambiente; distruzione o deterioramento di habitat all´interno di un sito protetto	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 356, 640, 640-bis, 640-ter c.p.);** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.);** **Art. 25-septies d.lgs 231/2001;** **Art. 25-octies d.lgs 231/2001** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (art. 316-ter);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 317, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis, 2638 c.c.);** **Art. 25-undecies d.lgs 231/2001 (artt. 452-bis, 452-quinquies, 733-bis c.p.)**

RUP per l'esecuzione del Progetto	Resp. funzione	Malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; falsità in documento pubblico informatico; accesso abusivo ad un sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione tra privati; istigazione alla corruzione tra privati; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; omicidio colposo e lesioni gravi o gravissime colpose - commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro; ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita; autoriciclaggio; inquinamento ambientale; delitti colposi contro l'ambiente; distruzione o deterioramento di habitat all'interno di un sito protetto	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 356, 640, 640-bis, 640-ter c.p.);** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.);** **Art 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 317, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis, 2638 c.c.);** **Art. 25-septies d.lgs 231/2001** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (art. 316-ter);** **Art. 25-octies d.lgs 231/2001;** **Art. 25-undecies d.lgs 231/2001 (artt. 452-bis, 452-quinquies, 733-bis c.p.)**
Monitoraggio della rete Wi-Fi nei confronti del Ministero competente e delle regioni	Resp. funzione	Falsità in documento pubblico informatico; accesso abusivo a sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; indebita percezione di erogazioni pubbliche; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione tra privati; istigazione alla corruzione tra privati; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; inquinamento ambientale; delitti colposi contro l'ambiente; distruzione o deterioramento di habitat all'interno di un sito protetto	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001(artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.);** **Art. 25 d.lgs. 231/2001 (artt. 317, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-ter, 640, 640-bis, 640-ter c.p.);** **Art. 24-bis d.lgs 231/2001 (artt.491-bis, 615-ter, 635-bis, 635-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316 c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis, 2638 c.c.);** **Art. 25-undecies d.lgs 231/2001 (artt. 452-bis, 452-quinquies, 733-bis c.p.)**

Gestione dei processi di sviluppo delle nuove tecnologie e servizi collegati alla rete WiFi e di tutti i servizi digitali	Resp. funzione	Falsità in documento pubblico informatico; accesso abusivo a sistema informatico o telematico; detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici; intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche; detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche; detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche; danneggiamento di informazioni, dati e programmi informatici, anche utilizzati dallo Stato o altro ente pubblico o comunque di pubblica utilità; danneggiamento di sistemi informatici o telematici; detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico; danneggiamento di sistemi informatici o telematici di pubblico interesse; messa a disposizione del pubblico di un'opera dell'ingegno protetta o di parte di essa; duplicazione abusiva di programmi per elaboratore; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori; riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati; abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere scientifiche; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa; omessa segnalazione alla Autorità giudiziaria o alla P.G. di condotte penalmente rilevanti ai sensi della L. n. 633/1941, degli artt. 615-ter e 640-ter c.p.; omessa comunicazione all'AGCOM di un punto di contatto diretto	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 615-quater, 617-quater, 617.quinquies, 635-bis, 635-ter, 635-quater, 635-quater.1, 635-quinquies c.p.);** **Art. 25-novies d.lgs 231/2001 (art. 171, 171-bis, 171-ter, 174-sexies L. n. 633/1941)**
Verifiche sul rispetto degli SLA per il piano WiFi	Resp. funzione	Frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; falsità in documento pubblico informatico; accesso abusivo ad un sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; frode nell'esercizio del commercio; vendita di prodotti industriali con segni mendaci; Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale; corruzione tra privati; istigazione alla corruzione tra privati; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (art. 640-ter c.p.);** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 356, 640, 640-bis c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 318, 319, 319-quater, 320, 322 c.p.);** **Art. 25-bis.1 (artt. 515, 517, 517-ter c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis, 2638 c.c.)**

Gestione della piattaforma WIFI Italia	Resp. funzione	Falsità in documento pubblico informatico; accesso abusivo a sistema informatico o telematico; detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici; intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche; detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche; detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche; danneggiamento di informazioni, dati e programmi informatici, anche utilizzati dallo Stato o altro ente pubblico o comunque di pubblica utilità; danneggiamento di sistemi informatici o telematici; detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico; danneggiamento di sistemi informatici o telematici di pubblico interesse; corruzione attiva e passiva; traffico di influenze illecite; messa a disposizione del pubblico di un'opera dell'ingegno protetta o di parte di essa; duplicazione abusiva di programmi per elaboratore; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori; riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati; abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere scientifiche; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa; omessa segnalazione alla Autorità giudiziaria o alla P.G. di condotte penalmente rilevanti ai sensi della L. n. 633/1941, degli artt. 615-ter e 640-ter c.p.; Omessa comunicazione all'AGCOM un punto di contatto diretto	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 615-quater, 617-quater, 617.quinquies, 635-bis, 635-ter, 635-quater, 635-quater.1, 635-quinquies c.p.);** **Art. 25-novies d.lgs 231/2001 (art. 171, 171-bis, 171-ter, 174-sexies L. n. 633/1941)**

V.4.6. ATTIVITÀ A RISCHIO E POTENZIALI REATI (PIANO ITALIA 5G BACKHAUL)

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Definizione della documentazione di as built (relazione tecnica, tracciato della rete, computo metrico e documentazione contabile) richiesta ai beneficiari per il completamento di ogni singolo intervento	Resp. piano	Frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; falsità in documento pubblico informatico; accesso abusivo a sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; impedito controllo; corruzione tra privati; istigazione alla corruzione tra privati; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; indebita percezione di erogazioni pubbliche; truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee; truffa aggravata per il conseguimento di erogazioni pubbliche; inquinamento ambientale; delitti colposi contro l'ambiente; dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti; dichiarazione fraudolenta mediante altri artifici; emissione di fatture o altri documenti per operazioni inesistenti; occultamento o distruzione di documenti contabili	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (art. 640-ter c.p.);** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 317, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis c.c.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-ter, 640, 640-bis, 640-ter c.p.);** **Art. 25-undecies (artt. 452-bis, 452-quinquies c.p.);** **Art. 25-quinquiesdecies d.lgs 231/2001 (artt. 2, 3, 8, 10 d.lgs 74/2000)**

Verifiche tecniche ed economiche sui lavori eseguiti attraverso il controllo della documentazione ed eventualmente attraverso controlli in situ su un campione di realizzazioni	Resp. piano, Team 5G, verificatori	indebita percezione di erogazioni pubbliche; falsità in documento pubblico informatico; accesso abusivo a sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; impedito controllo; corruzione tra privati; istigazione alla corruzione tra privati; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; omicidio colposo e lesioni gravi o gravissime colpose - commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro; malversazione di erogazioni pubbliche; truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita; autoriciclaggio; inquinamento ambientale; delitti colposi contro l'ambiente; dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti; dichiarazione fraudolenta mediante altri artifici; emissione di fatture o altri documenti per operazioni inesistenti; occultamento o distruzione di documenti contabili	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (art. 640-ter c.p.);** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 317, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2625, 2635, 2635-bis, 2638 c.c.);** **Art. 25-septies d.lgs 231/2001** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 356, 640, 640-bis, 640-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 318, 319, 319-quater, 320, 322 c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis, 2638 c.c.);** **Art. 25-octies d.lgs 231/2001;** **Art. 25-undecies (artt. 452-bis, 452-quinquies c.p.);** **Art. 25-quinquiesdecies d.lgs 231/2001 (artt. 2, 3, 8, 10 d.lgs 74/2000)**
Gestione di eventuali criticità relative alle autorizzazioni con Enti privati e pubblici	Resp. piano/Resp. RMC	Frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; falsità in documento pubblico informatico; accesso abusivo a sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; impedito controllo; corruzione tra privati; istigazione alla corruzione tra privati; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; inquinamento ambientale; delitti colposi contro l'ambiente; distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici; devastazione e saccheggio di beni culturali e paesaggistici	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (art. 640-ter);** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 317, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2625, 2635, 2635-bis, 2638 c.c.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 640, 640-bis c.p.);** **Art. 25-undecies (artt. 452-bis, 452-quinquies c.p.);** **Art. 25-septies-decies (artt. 518-duodecies c.p.);** **Art. 25-duodevicies (art. 518-terdecies c.p.)**

Coordinamento, in collaborazione con il Dipartimento per la Trasformazione Digitale, per le attività di monitoraggio delle milestone previste dal PNRR e per la divulgazione dei contenuti tecnici del Piano verso gli Enti e le Regioni	Resp. piano/Resp. RMC/D.G./A.D.	Falsità in documento pubblico informatico; accesso abusivo a sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione attiva o passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; induzione indebita a dare o promettere utilità, corruzione attiva e passiva, corruzione in atti giudiziari e istigazione alla corruzione - di membri degli organi UE o di funzionari UE; traffico di influenze illecite; corruzione tra privati; istigazione alla corruzione tra privati; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; abuso o comunicazione illecita di informazioni privilegiate - raccomandazione o induzione di altri alla commissione di abuso di informazioni privilegiate	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 356, 640, 640-bis, 640-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 318, 319, 319-quater, 320, 321, 322, 322-bis, 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis, 2638 c.c.);** **Art. 25-sexies d.lgs 231/2001 (art. 184 TUF)**

V.4.7. ULTERIORI ELEMENTI DI CONTROLLO PER PIANO ITALIA 5G BACKHAUL

Tra le responsabilità dell'unità organizzativa Piano Italia 5G Backhaul vi è quella della Analisi delle criticità e fornitura di chiarimenti operativi sia tecnici che di processo, anche avvalendosi del supporto del Dipartimento per la Trasformazione digitale.
Nella mappatura dei rischi tale attività risulta meramente strumentale, in quanto consiste in attività di supporto, coordinamento e monitoraggio priva di un significativo margine di esposizione. Tuttavia, non si può escludere che una grave carenza nel suo svolgimento possa agevolare od occultare la commissione di un illecito, né, altresì, può escludersi che i responsabili di tale funzione partecipino in concorso con le funzioni coinvolte in altre ipotesi di rischio, divenendo in tal caso essi stessi direttamente autori dell'illecito.
Di seguito il riepilogo delle attività meramente strumentali:

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Analisi delle criticità e fornitura di chiarimenti operativi sia tecnici che di processo, anche avvalendosi del supporto del Dipartimento per la Trasformazione digitale	Resp. piano	Frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; falsità in documento pubblico informatico; accesso abusivo a sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; inquinamento ambientale; delitti colposi contro l'ambiente; distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici; devastazione e saccheggio di beni culturali e paesaggistici	**RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (art. 640-ter c.p.);** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.);** **Art. 25-undecies (artt. 452-bis, 452-quinquies c.p.);** **Art. 25-septiesdecies (artt. 518-duodecies c.p.);** **Art. 25-duodevicies (art. 518-terdecies c.p.)**
Definizione degli step operativi di verifica e controllo dei lavori inerenti al piano attraverso procedure operative e check-list di controllo;	Resp. piano/Resp. RMC	indebita percezione di erogazioni pubbliche; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; falsità in documento pubblico informatico; accesso abusivo a sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; omicidio colposo e lesioni gravi o gravissime colpose - commessi con violazione delle norme	**RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt, 316-ter, 640, 640-bis, 640-ter c.p.);** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.);** **Art. 25-septies d.lgs 231/2001**

		sulla tutela della salute e sicurezza sul lavoro	

Al fine di prevenire gli ulteriori rischi di illecito correlati a queste attività meramente strumentali, il *risk owner* di primo livello svolge la propria attività in coordinamento con le altre funzioni interne e della Capogruppo coinvolte, rispettando i principi generali di controllo e il codice etico, avendo come punti di attenzione i rischi strumentali sopra indicati.
Il process owner garantisce l'effettività e l'efficacia dei controlli, adeguando periodicamente le procedure. A tal fine richiede una informativa ai risk owner, sulla base della quale egli acquisisce le informazioni rilevanti per attuare le opportune azioni correttive e alimentare i flussi informativi, segnalando tempestivamente all'OdV, e al RPCT se di competenza, eventuali anomalie o non conformità riscontrate.

V.4.8. ATTIVITÀ A RISCHIO E POTENZIALI REATI (SCUOLE CONNESSE)

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Collaudi degli interventi previsti per il collegamento in fibra delle scuole italiane e manutenzione per singola sede scolastica	Resp. funzione	Malversazione di erogazioni pubbliche; frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; falsità in documento pubblico informatico; accesso abusivo ad un sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; omicidio colposo e lesioni gravi o gravissime colpose - commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro; indebita percezione di erogazioni pubbliche; corruzione tra privati; istigazione alla corruzione tra privati; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita; autoriciclaggio; inquinamento ambientale; delitti colposi contro l'ambiente; distruzione o deterioramento di habitat all'interno di un sito protetto	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 356, 640, 640-bis, 640-ter);** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 317, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25-septies d.lgs 231/2001** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (art. 316-ter);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 317, 318, 319, 319-quater, 320, 321, 322 c.p., 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis, 2638 c.c.);** **Art. 25-septies d.lgs 231/2001;** **Art. 25-octies d.lgs 231/2001;** **Art. 25-undecies d.lgs 231/2001 (artt. 452-bis, 452-quinquies, 733-bis c.p.)**

RUP per l'esecuzione del progetto	Resp. funzione	Malversazione di erogazioni pubbliche; frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; falsità in documento pubblico informatico; accesso abusivo ad un sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione tra privati; istigazione alla corruzione tra privati; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; rifiuto d'atti d'ufficio. omissione indebita percezione di erogazioni pubbliche; omicidio colposo e lesioni gravi o gravissime colpose - commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro; ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita; autoriciclaggio; inquinamento ambientale; delitti colposi contro l'ambiente; distruzione o deterioramento di habitat all'interno di un sito protetto	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 356, 640, 640-bis, 640-ter c.p.);** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 317, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis, 2638 c.c.)** **L. 190/2012 (art. 328 c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (art. 316-ter c.p.);** **Art. 25-septies d.lgs 231/2001;** **Art. 25-octies d.lgs 231/2001;** **Art. 25-undecies d.lgs 231/2001 (artt. 452-bis, 452-quinquies, 733-bis c.p.)**
Gestione dei rapporti con i Gruppi di Lavoro per la raccolta degli elementi utili alla redazione dei Piani Tecnici	Resp. funzione	Falsità in documento pubblico informatico; accesso abusivo ad un sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 317, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (art. 640, 640-bis, 640-ter c.p.)**
Redazione dei Piani tecnici per la pianificazione e la progettazione degli interventi relative alle diverse strutture scolastiche	Resp. funzione	Falsità in documento pubblico informatico; malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; accesso abusivo ad un sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione tra privati; istigazione alla corruzione tra privati; inquinamento ambientale; delitti colposi contro l'ambiente;	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis c.p.);** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 640, 640-bis, 640-ter c.p.);** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 317, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (art. 2635, 2635-bis c.c.);** **Art. 25-undecies d.lgs 231/2001 (artt. 452-bis, 452-quinquies c.p.)**

Monitoraggio del rispetto degli SLA contrattuali relativi ai servizi attivati dalle strutture scolastiche	Resp. funzione	Frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; falsità in documento pubblico informatico; accesso abusivo ad un sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione tra privati; istigazione alla corruzione tra privati; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (art. 640-ter c.p.);** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 356, 640, 640-bis c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 318, 319, 320, 322 c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis, 2638 c.c.)**
Verifiche tecniche ed economiche sui lavori eseguiti attraverso il controllo della documentazione ed eventualmente attraverso controlli in situ su un campione di realizzazioni	Resp. funzione	Falsità in documento pubblico informatico; accesso abusivo ad un sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione tra privati; istigazione alla corruzione tra privati; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; omicidio colposo e lesioni gravi o gravissime colpose - commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro; malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita; autoriciclaggio; inquinamento ambientale; delitti colposi contro l'ambiente; dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti; dichiarazione fraudolenta mediante altri artifici; emissione di fatture o altri documenti per operazioni inesistenti; occultamento o distruzione di documenti contabili	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 318, 319, 319-quater, 320, 322 c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis, 2638 c.c.);** **Art. 25-septies d.lgs 231/2001;** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 356, 640, 640-bis, 640-ter c.p.);** **Art. 25-octies d.lgs 231/2001;** **Art. 25-undecies d.lgs 231/2001 (artt. 452-bis, 452-quinquies c.p.);** **Art. 25-quinquiesdecies d.lgs 231/2001 (artt. 2, 3, 8, 10 d.lgs 74/2000)**
Coordinamento con il Dipartimento del MITD per le attività di monitoraggio delle milestone previste dal PNRR e per la divulgazione dei contenuti tecnici del Piano verso i distretti scolastici e le Regioni	Resp. funzione/Resp.RMC/D.G./A.D.	Falsità in documento pubblico informatico; accesso abusivo ad un sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; Abuso o comunicazione illecita di informazioni privilegiate. Raccomandazione o induzione di altri alla commissione di abuso di informazioni privilegiate	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 356, 640, 640-bis, 640-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (art. 2638 c.c.);** **Art. 25-sexies d.lgs 231/2001 (art. 184 TUF)**

Esecuzione delle attività definite nel Piano Operativo "Scuola Connessa fase 2" compreso nell'investimento "Reti ultraveloci" del PNRR	Resp. funzione	Frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; accesso abusivo ad un sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; omicidio colposo e lesioni gravi o gravissime colpose - commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro; malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee; truffa aggravata per il conseguimento di erogazioni pubbliche; indebita destinazione di denaro o cose mobili offensiva degli interessi finanziari dell'UE; ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita; autoriciclaggio; inquinamento ambientale; delitti colposi contro l'ambiente	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (art. 640-ter c.p.);** **Art. 24-bis d.lgs 231/2001 (artt. 615-ter, 635-bis, 635-ter c.p.);** **Art. 25-septies d.lgs 231/2001** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt.316-bis, 316-ter, 640, 640-bis c.p.);** **Art. 25 d.lgs 231/2001 (art. 314-bis);** **Art. 25-octies d.lgs 231/2001;** **Art. 25-undecies d.lgs 231/2001 (artt. 452-bis, 452-quinquies c.p.)**

V.4.9. ULTERIORI ELEMENTI DI CONTROLLO PER SCUOLE CONNESSE

Tra le responsabilità dell'unità organizzativa Piano Scuole Connesse vi è quella dell'analisi della Progettazione e sviluppo degli interventi previsti per il collegamento in fibra delle scuole italiane.
Nella mappatura dei rischi tale attività risulta meramente strumentale, in quanto consiste in attività di supporto preliminarepriva di un significativo margine di esposizione. Tuttavia, non si può escludere che una grave carenza nel suo svolgimento possa agevolare od occultare la commissione di un illecito, né, altresì, può escludersi che i responsabili di tale funzione partecipino in concorso con le funzioni coinvolte in altre ipotesi di rischio, divenendo in tal caso essi stessi direttamente autori dell'illecito.
Di seguito il riepilogo delle attività meramente strumentali:

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Progettazione e sviluppo degli interventi previsti per il collegamento in fibra delle scuole italiane	Resp. funzione	Indebita percezione di erogazioni pubbliche; falsità in documento pubblico informatico; accesso abusivo a sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione tra privati; istigazione alla corruzione tra privati; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita; autoriciclaggio; messa a disposizione del pubblico di un'opera dell'ingegno protetta o di parte di essa; duplicazione abusiva di programmi per elaboratore; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori; riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati; inquinamento ambientale; delitti colposi contro l'ambiente; distruzione o deterioramento di habitat all'interno di un sito protetto	**RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (art. 316-ter);** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 317, 318, 319, 319-quater, 320, 321, 322 c.p., 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis, 2638 c.c.);** **Art. 25-octies d.lgs 231/2001;** **Art. 25-novies d.lgs 231/2001 (artt. 171, 171-bis L. n. 633/1941);** **Art. 25-undecies d.lgs 231/2001 (artt. 452-bis, 452-quinquies, 733-bis c.p.)**

Al fine di prevenire gli ulteriori rischi di illecito correlati a questa attività meramente strumentali, il *risk owner* di primo livello svolge la propria attività in coordinamento con le altre funzioni interne e della Capogruppo coinvolte, rispettando i principi generali di controllo e il codice etico, avendo come punti di attenzione i rischi strumentali sopra indicati.
Il process owner garantisce l'effettività e l'efficacia dei controlli, adeguando periodicamente le procedure. A tal

fine richiede una informativa ai risk owner, sulla base della quale egli acquisisce le informazioni rilevanti per attuare le opportune azioni correttive e alimentare i flussi informativi, segnalando tempestivamente all'OdV, e al RPCT se di competenza, eventuali anomalie o non conformità riscontrate.

V.4.10. ELEMENTI DI CONTROLLO PER L'ATTUAZIONE DEI PIANI PNRR (SCUOLE CONNESSE, SANITÀ CONNESSA, PIANO ITALIA 5G) E GESTIONE DELLE ALTRE COMMESSE.

Le attività delle aree **a rischio Reti Mobili e Connettività** e i relativi elementi di controllo si riferiscono a tutte le unità organizzative cui compete la realizzazione e l'attuazione degli interventi mediante affidamento diretto (Scuole Connesse, Sanità Connessa), e incentivo (Italia 5 Giga Backhaul).

Le attività sensibili sono state identificate per singolo Ufficio e gli elementi di controllo sono comuni a tutti gli Uffici che compongono l'Area a rischio Reti Mobili e Connettività.

Infratel Italia assicura che le attività di progettazione e realizzazione delle infrastrutture di rete siano condotte in maniera corretta, trasparente e tracciabile, nel rispetto delle condizioni previste dal contratto/convenzione stipulati con il committente e della normativa vigente e applicabile alla Società.

Preliminarmente, è scelto ilRUP per l'esecuzione del progetto tra i responsabili degli uffici coinvolti, nel rispetto delle misure organizzative e dei requisiti di legge, conformemente a quanto previsto per l'unità Pianificazione, Gare e Ingegneria, al paragrafo "Svolgimento del ruolo di RUP per tutti i procedimenti di affidamento per il rispetto degli adempimenti normativi e del sistema di e-procurement".

I Responsabili degli Uffici propongono l'organigramma di commessa/progetto, nel quale sono indicati il Responsabile di commessa e il RUP oltre agli altri adempimenti previsti specificamente dalla normativa sui contratti pubblici, ivi inclusa la dichiarazione sul conflitto di interessi, nonché tutte le risorse costituenti il team di commessa/progetto e lo sottopongono per approvazione all'Amministratore Delegato. L'Ufficio Risorse Umane provvede a comunicare l'organigramma, approvato dall'Amministratore delegato, a tutti i soggetti/Uffici interessati, attraverso la pubblicazione sulla intranet aziendale.

Infratel Italia assicura la regolare esecuzione delle attività svolte (attività di commessa o progetto), nel rispetto di quanto previsto nel contratto/convenzione e nel Piano associato.

Le commesse sono scandite per fasi da suddividersi almeno nelle seguenti: apertura commessa; programmazione e avvio; gestione e controlli; rendicontazione; chiusura commessa. L'ufficio, nelle fasi preliminari, si coordina con l'unità Pianificazione, Gare e ingegneria per definire l'accordo di programma/convenzione con INF o con le Regioni e il relativo piano operativo e gli adempimenti di gara. Le fasi devono essere distribuite secondo i principi di segregazione dei ruoli e diffusione dei controlli.

Il Responsabile di commessa e il RUP in collaborazione con la funzione Legale di Capogruppo, o a quella Legale interna Controllo Operativo PNRR, per quanto di competenza e con Verifiche Cantieri, anche per le opportune verifiche di qualità e SSL, sono tenuti a monitorare il rispetto del Piano operativo, comunicando eventuali varianti, scostamenti o anomalie all'Ufficio competente per la definizione di opportune azioni, da comunicare, se necessario, all'Ufficio Pianificazione Gare e Ingegneria.

Il Responsabile di commessa/RUP assicura, nel rispetto del Piano operativo, la realizzazione (nel caso di affidamenti diretti) o l'acquisizione dal concessionario (nel caso di concessioni) della progettazione preliminare/definitiva/esecutiva, corredata dei documenti previsti dalla norma di riferimento, e la sottopone al Responsabile dell'Ufficio per l'approvazione. Comunica formalmente all'appaltatore l'avvenuta approvazione della progettazione. Il Responsabile di Commessa/RUP deve inoltre monitorare, evidenziando al Responsabile dell'Ufficio eventuali scostamenti, il rispetto dei tempi previsti dai contratti di appalto o di concessione.

Con specifico riferimento al modello "incentivo", durante le fasi di esecuzione lavori sono svolte le verifiche tecniche in merito allo stato delle attività tramite report di avanzamento, trasmessi dal beneficiario, ed eventuali sopralluoghi, per mezzo di un verbale di sopralluogo sul cantiere effettuati dal personale di Infratel Italia, formalizzati attraverso la compilazione di opportuna documentazione preliminarmente predisposta. I controlli possono essere svolti mediante verifiche *in situ* a campione e/o tramite video ispezioni da remoto, nonché mediante altri controlli tecnici adeguati in termini di affidabilità, con altri mezzi tecnologici. I report sono tracciati tramite il sistema informativo di gestione commesse/progetti o altro strumento equivalente con i dati relativi all'avanzamento delle attività. Deve inoltre essere garantita segregazione funzionale tra chi contribuisce all'elaborazione della documentazione di supporto alle attività di monitoraggio e controllo e chi svolge le attività di attuazione e gestione.

Il Responsabile di Commessa/Progetto, con il supporto dell'Ufficio Rendicontazione, assicura, sulla base delle scadenze previste dal contratto/convenzione, l'attuazione delle attività preordinate al processo di rendicontazione verso il committente nel rispetto dei codici di condotta e degli elementi di controllo relativi al processo di Rendicontazione stabiliti nel presente documento.

Le attività di monitoraggio della commessa/progetto sono svolte periodicamente dall'Ufficio competente. Qualora si verifichi un evento straordinario in grado di incidere sul budget complessivo di commessa/progetto e di conseguenza sul Piano operativo, il Responsabile di commessa/progetto valuta di concerto con l'Ufficio competente e informando l'Amministratore Delegato se coinvolgere i comitati di controllo preposti, ove esistenti, chiamati a sovraintendere il monitoraggio della commessa.

Il Responsabile di Commessa/RUP, con il supporto di Rendicontazione, assicura, sulla base delle scadenze previste dal contratto/convenzione, l'attuazione delle attività preordinate al processo di rendicontazione nel rispetto dei codici di condotta e degli elementi di controllo relativi al processo di rendicontazione stabiliti nel presente documento.

In fase di chiusura della commessa/progetto, il Responsabile di commessa/progetto attesta l'effettivo completamento delle attività e la corretta produzione dei documenti di commessa/progetto in un rapporto finale di chiusura commessa/progetto. Tale rapporto viene sottoposto a validazione e firma da parte dell'Ufficio competente e, qualora previsto, del committente per l'attestazione di regolare esecuzione.

Devono essere **verbalizzate le attività di gestione della commessa/progetto** che prevedono **comunicazioni e/o incontri formali** con soggetti rappresentanti del committente, ad esempio in occasione della condivisione/approvazione di Stati Avanzamento Lavori o di prospetti rendicontativi.

Infratel Italia elabora dati accurati sulla presenza del personale aziendale impegnato nelle varie commesse/progetti, anche per mezzo di sistemi di rilevazione - timbratura badge, timesheet ed applicativi dedicati. Il personale è tenuto, utilizzando gli applicativi dedicati, attraverso le modalità e nel rispetto delle scadenze definite e comunicate dalla funzione Risorse Umane (svolta in service dalla Capogruppo), dunque **sulla base delle linee guida di Capogruppo** ed in coordinamento con le competenti funzioni della stessa, ad aggiornare costantemente la situazione presenze, inserendo in modo corretto e veritiero i giustificativi di presenza/assenza occorrenti alla quadratura periodica.

I soggetti preposti all'approvazione delle presenze/assenze del personale autorizzano le presenze/assenze richieste dalle risorse e sono tenuti a verificare ed approvare i dati disponibili a sistema secondo le modalità e le scadenze definite e comunicate dalla funzione Risorse Umane presso la Capogruppo. Quest'ultima provvede, sulla base dei dati e dell'iter autorizzativo posto in essere, all'esatta contabilizzazione delle presenze/assenze del personale.

Il Referente di Contratto di Servizio/Amministratore Delegato garantisce il rispetto delle attività espletate dalla Capogruppo.

Infratel Italia elabora dati accurati relativi alle attività lavorative effettivamente svolte sulle commesse/progetti, interne od esterne, in termini di ore lavorate dal personale aziendale anche attraverso l'impiego di idonei sistemi informatici dedicati. Gli Uffici a cui riferiscono i Responsabili di commessa/RUP competenti eseguono le opportune **verifiche dell'effettiva presenza del personale nei giorni di lavoro caricati a sistema e consuntivati sulla commessa/progetto**, anche attraverso la verifica periodica, almeno su base mensile, di coerenza tra le presenze/assenze del personale e le trasferte pianificate/consuntivate.

L'Amministratore Delegato, **avvalendosi della collaborazione della funzione Controllo di Gestione**, **stabilisce le opportune modalità operative per l'imputazione delle ore lavorate su ciascuna Commessa/Progetto** al fine di consentire l'esatta attribuzione dei costi rendicontabili al committente.

Il sistema informativo e di comunicazione di Infratel Italia **assicura** che l'**attribuzione** del tempo lavorato su ciascuna commessa/progetto sia **corretta e condivisa** dalle risorse direttamente coinvolte e **dai** Soggetti titolati alla verifica e approvazione, ossia i **Responsabili di Commessa/RUP**, **nonché** tempestiva per **il consolidamento dei dati contabili** e strumentali alla rendicontazione verso il committente. Il personale è tenuto alla corretta, veritiera e coerente imputazione del tempo effettivamente lavorato su ciascuna commessa/progetto aziendale, interna e/o esterna, utilizzando gli applicativi dedicati, attraverso le modalità operative stabilite e nel rispetto delle scadenze definite dall'Ufficio Controllo di Gestione.

I Responsabili preposti alla verifica del tempo lavorato sulla commessa/progetto sono tenuti a verificare, approvare o respingere quanto imputato dalle risorse, attraverso le modalità operative stabilite e nel rispetto delle scadenze definite. Eventuali errori accertati dovranno essere segnalati dal Responsabile e quindi corretti dalla risorsa interessata.

Infratel Italia assicura correttezza, trasparenza e tracciabilità nella gestione delle trasferte lavorative del proprio personale.

Le **trasferte** sono preliminarmente **pianificate dai Responsabili di Commessa/RUP** in relazione alle commesse di propria responsabilità. **Ciascuna trasferta**, per la quale deve sempre essere identificata la **commessa interna e/o esterna di riferimento**, viene richiesta dai soggetti interessati e sottoposta **all'approvazione del proprio Responsabile o del Responsabile di Commessa se diverso**.

Le risorse interessate sono tenute alla corretta **rendicontazione delle spese sostenute** per la trasferta nel rispetto delle voci di spesa rimborsabili **definite in apposite policies interne, anche di gruppo**, attraverso la predisposizione di una nota spese, a cui devono essere allegati i relativi giustificativi fiscalmente validi, oggetto di verifica ed autorizzazione da parte dei Responsabili di Commessa/RUP.

La funzione Amministrazione e Bilancio presso la Capogruppo è tenuta ad effettuare il controllo dei rapporti e dei giustificativi verificando il rispetto delle policies aziendali e di gruppo.

In fase di chiusura dell'intervento, il Responsabile di commessa/RUP attesta l'effettivo completamento delle attività e la corretta produzione dei documenti di commessa in un rapporto finale di chiusura commessa. Tale rapporto viene sottoposto a validazione e firma da parte del Responsabile dell'Ufficio e, qualora previsto, del committente per l'attestazione di regolare esecuzione.

Nel caso in cui siti di pertinenza di Infratel Italia siano sottoposti a sequestro, la funzione competente, ovvero il soggetto interno, formalmente identificato/incaricato dai Soggetti titolati della Società, a cui è affidata la custodia dei siti stessi, è tenuto, affinché ne sia preservata l'integrità, a prendere i dovuti provvedimenti atti a limitare l'accesso all'area sottoposta a sequestro al solo personale preventivamente autorizzato, anche tramite

la segregazione della stessa per mezzo di opportuni dispositivi e l'apposizione di idonea segnaletica. Se ad essere sottoposti a sequestro sono beni mobili di proprietà aziendale, o comunque affidati in custodia alla Società, ovvero presenti in siti di sua pertinenza, la funzione competente, ovvero il referente interno, formalmente identificato/incaricato dai Soggetti titolati della Società, a cui è affidata la custodia degli stessi, è tenuto a prendere i dovuti provvedimenti al fine di impedirne l'uso, il danneggiamento o la sottrazione, anche tramite la segregazione dei beni confiscati per mezzo di opportuni dispositivi e l'apposizione di idonea segnaletica.

È fatto divieto a tutto il personale interessato alle attività in esame di appropriarsi indebitamente, anche temporaneamente, di materiali, beni e strumentazione della Società o di terzi.

Per quanto concerne l'attuazione dei piani a incentivo, la Società attua un programma di controlli sul beneficiario privato (a campione *in situ* o da remoto, con soluzioni tecniche adeguate) e prevede specifiche clausole risolutive contrattuali, per la violazione del MOGC 231.

V.4.10.1. Servizi digitali

Oltre alle commesse finalizzate alla progettazione, la realizzazione e la gestione di reti ed infrastrutture a banda ultralarga, Infratel Italia gestisce anche commesse finalizzate alla fornitura di servizi digitali per la pubblica amministrazione, che connotano Infratel Italia come Service Provider. Per questa tipologia di commesse la rete si configura come la fornitura di un servizio chiavi in mano e non prevede il coinvolgimento di Infratel Italia nella conduzione e la responsabilità dei lavori.

Per il controllo delle commesse/progetti per la fornitura di servizi, oltre al RUP e al Responsabile di Commessa/Progetto la normativa di riferimento prevede il Direttore dell'Esecuzione per gli appalti di servizi e fornitura con importo superiore a 500.000 euro. Il Direttore dell'Esecuzione riceve dal RUP le disposizioni per garantire la regolarità e il controllo tecnico-contabile dell'esecuzione del contratto di fornitura, impartisce all'appaltatore le disposizioni operative attraverso ordini di servizio e redige i verbali di accertamento e le relazioni periodiche sull'avanzamento delle principali attività di esecuzione del contratto che devono essere inviati al RUP.

V.4.10.2. Scuole Connesse

Una delle commesse per la fornitura di servizi è la commessa "Scuole Connesse".

Il Responsabile del Piano Scuole Connesse cura direttamente tramite il Direttore dell'Esecuzione i rapporti con gli appaltatori individuati per la fase di esecuzione della fornitura e fornisce le informazioni relative alla commessa e collabora con le altre funzioni aziendali coinvolte nella gestione della commessa.

La progettazione è a cura dell'appaltatore, che realizza il progetto di connessione per l'esecuzione della fornitura nella singola scuola e lo consegna ad Infratel Italia per la verifica e l'approvazione attraverso le piattaforme tecnologiche a ciò dedicate (piattaforma Geo4Wip). Il Direttore dell'Esecuzione garantisce, attraverso i progettisti interni, la conformità del progetto alle norme tecniche e ai requisiti contrattuali.

Il Progettista interno verifica la progettazione ricevuta dall'appaltatore e in caso di esito positivo approva il progetto di connessione e genera l'emissione di un Ordine di Intervento che viene sottoposto alla firma del RUP e trasmesso all'appaltatore. In caso di esito negativo della verifica, il progetto viene rifiutato invitando l'appaltatore a rettificare e/o integrare il progetto.

Il Direttore dell'Esecuzione verifica lo stato di avanzamento dell'esecuzione della fornitura monitorando mensilmente il numero delle attivazioni del servizio realizzate dall'appaltatore, evidenziando al RUP eventuali criticità. L'appaltatore trasmette mensilmente l'elenco delle scuole attivate nel mese precedente.

Dopo aver eseguito e completato l'esecuzione dell'Ordine di intervento, l'appaltatore consegna a Infratel la documentazione di collaudo, il Verbale di Attivazione e il report dello *speed test* eseguito nella scuola per testare il servizio di connettività. Il Progettista interno verifica la documentazione di collaudo fornita e in caso di esito positivo convalida su Geo4Wip la data di attivazione del servizio. In caso di esito negativo la documentazione viene rifiutata dal Progettista interno, richiedendo eventuali modifiche e/o integrazioni.

Una volta convalidata la data di attivazione, l'appaltatore può procedere con la consegna su Geo4Wip della documentazione di *as-built*. Il Progettista verifica la suddetta documentazione e in caso di esito positivo la approva emettendo, in collaborazione con il Direttore dell'Esecuzione, il Verbale di Regolare esecuzione. In caso di esito negativo della verifica la documentazione viene rifiutata dal Progettista richiedendo all'APP eventuali modifiche e/o integrazioni.

Il SAL viene verificato dal Direttore dell'Esecuzione e su richiesta del Responsabile di Commessa approvato e firmato dal RUP, che emette anche il benestare al pagamento.

Per l'esecuzione delle funzioni di controllo, il Direttore dell'Esecuzione effettua, in collaborazione col Responsabile di Commessa/Progetto, campagne trimestrali di accertamento e verifica in campo della regolarità della fornitura. Gli accertamenti sono effettuati su un campione selezionato di scuole appartenenti al perimetro di gara sulla base di un'istruzione operativa appositamente definita.

Inoltre, il Direttore dell'Esecuzione controlla e monitora attraverso i sistemi di preposti il rispetto degli SLA contrattuali per la gestione degli interventi di assistenza tecnica e manutenzione del servizio di connettività, della rete e degli apparati di accesso per l'intera durata della fornitura.

Le altre attività della commessa/progetto, la rendicontazione, i pagamenti, gli incassi e la chiusura di commessa sono gestiti come per le altre commesse dal Responsabile di Commessa/Progetto e dalle funzioni Rendicontazione e Amministrazione e Bilancio.

Qualora si verifichi un evento straordinario o comunque in grado di incidere sul budget complessivo e/o sul Piano Tecnico, il Responsabile di Commessa/Progetto coinvolge le funzioni competenti per la valutazione di una modifica del Piano Tecnico che deve essere approvata dagli organi di controllo preposti al monitoraggio della commessa (comitati di controllo e monitoraggio). Una volta approvata la modifica del PT, seguirà una nuova versione del Piano Operativo di Commessa/Progetto.

V.4.10.3. Manutenzione Wi-Fi

Infratel Italia assicura che le attività di **manutenzione delle infrastrutture wi-fi** siano condotte in maniera corretta, trasparente e tracciabile, nel rispetto delle condizioni previste dagli accordi stipulati e della normativa vigente e applicabile alla Società.

Per ogni attività di manutenzione è individuato un Responsabile di commessa di manutenzione/RUP (di seguito anche "Manutenzione").

La risoluzione di anomalie viene svolta direttamente da personale di Infratel Italia, a seguito di segnalazione da parte dell'Ente, oppure mediante interventi per il tramite del fornitore incaricato, qualora non sia possibile risolvere il guasto diversamente.

Le attività di manutenzione sono affidate al fornitore incaricato nell'ambito di un accordo quadro o di altra procedura di affidamento, ovvero di gara, in aderenza alle soglie di rilevanza ai sensi del codice del contratti pubblici.

Si osservano, per quanto di competenza, i protocolli relativi al paragrafo "Elementi di controllo per Gestione Rete".

V.4.10.4. Voucher

Per quanto attiene al progetto Voucher, valgono i principi espressi per le aree trasversali, con specifico riferimento alla gestione dei finanziamenti/fondi.

Sono inoltre previsti specifici controlli per l'accreditamento degli operatori che devono iscriversi in un apposito elenco (art. 6, comma 1 del decreto ministeriale).

La registrazione nell'elenco è subordinata al buon esito delle verifiche effettuate da Infratel Italia e dal RUP.

Nello specifico, l'Operatore telefonico interessato dovrà fornire la documentazione necessaria del "Manuale operativo voucher imprese".

Ai fini dell'iscrizione in elenco, gli operatori devono dichiarare di essere in possesso dei titoli necessari per l'erogazione dei servizi di comunicazione, di non versare in nessuna delle situazioni di cui agli artt. 94, 95, 96 e 97 del D.lgs. n. 36/2023.

È fatto divieto a tutto il personale interessato alle attività in esame di appropriarsi indebitamente, anche temporaneamente, di materiali/strumentazioni della Società o di terzi.

Tutti gli attori coinvolti hanno l'obbligo di comunicare tempestivamente all'Organismo di Vigilanza deroghe, anomalie o atipicità eventualmente riscontrate rispetto alle determinazioni stabilite per il presente processo.

I responsabili di tutti gli Uffici sotto la responsabilità dell'unità Reti Mobili e Connettività sono tenuti, ciascuno per gli interventi di propria competenza, alla comunicazione periodica, su base semestrale, all'Organismo di Vigilanza, al RPCT, al Direttore Generale e all'Amministratore Delegato di un'informativa sullo stato di avanzamento d ciascuna commessa/progetto/piano e delle verifiche effettuate.

Fermo restando l'obbligo in capo a tutti gli attori coinvolti, il RUP (scelto tra i diversi responsabili degli Uffici a seconda dell'ambito in cui rientra l'intervento) è, inoltre, tenuto alla comunicazione periodica, su base annuale, di un'informativa riepilogativa all'Organismo di Vigilanza, al RPCT, al Direttore Generale e all'Amministratore Delegato, delle varianti approvate nel periodo di riferimento con l'indicazione dell'importo, delle motivazioni e dei soggetti beneficiari con l'indicazione delle eventuali azioni correttive stabilite.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate, gli Uffici dell'Area Reti Mobili e Connettività, insieme all'Ufficio Controllo di Gestione, sono tenuti alla comunicazione periodica, su base annuale all'OdV, al RPCT, al Direttore Generale e all'Amministratore Delegato di un'informativa riepilogativa del tempo effettivamente lavorato su ciascuna commessa/progetto/piano aziendale da risorse interne.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate all'Organismo di Vigilanza ed al RPCT, l'Ufficio wi-fi e Servizi Digitali è inoltre tenuto alla comunicazione periodica, su base annuale, di un'informativa riepilogativa dei dati relativi al servizio di manutenzione e dell'esito delle attività di verifica a campione sull'operato delle ditte di manutenzione con l'indicazione delle eventuali azioni correttive stabilite.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate all'Organismo di Vigilanza ed al RPCT, l'Ufficio Voucher è inoltre tenuto alla comunicazione periodica, su base annuale, di un'informativa riepilogativa dei dati relativi ai controlli effettuati sui voucher prenotati ed erogati.

In ogni caso, il responsabile di ciascun Ufficio dell'Area Reti Mobili e Connettività comunica all'OdV e al RPCT, con cadenza almeno annuale, le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

V.5 INFRASTRUTTURE E OPERATIONS

L'unità organizzativa "Infrastrutture e Operations" si occupa delle "commesse" (o progetti e piani) relative al servizio di realizzazione, gestione e manutenzione delle infrastrutture di rete fissa, gestendo in particolare: le operazioni da attuare secondo i modelli "a concessione", "a incentivo" e "a intervento diretto"; gestisce inoltre, attraverso le unità a ciò dedicate, lo sviluppo, l'alimentazione e la manutenzione della banca dati SINFI (catasto delle infrastrutture), lo sviluppo del business (in particolare per le attività di cessione dei diritti per lo sfruttamento delle infrastrutture), le verifiche tecniche ed esecutive per i lavori di realizzazione degli interventi finanziati; il processo di acquisizione di infrastrutture; la manutenzione, il delivery e lo sviluppo della rete.

V.5.1. ATTIVITÀ A RISCHIO E POTENZIALI REATI (INFRASTRUTTURE E OPERATIONS)

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Funzione di RUP	Resp. funzione, Soggetti legittimati	Falsità in documento pubblico informatico; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione attiva o passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione e istigazione alla corruzione tra privati; omicidio o lesioni gravi e gravissime aggravati dalla violazione delle norme sulla prevenzione degli infortuni sul lavoro e delle malattie professionali; riciclaggio o rempiego in attività produttive di beni di provenienza illecita; rifiuto d'atti d'ufficio. omissione malversazione di beni pubblici; frode nelle pubbliche forniture; truffe, anche informatiche, ai danni di PA centrali o locali; inquinamento ambientale; disastro ambientale; delitti colposi contro l'ambiente; distruzione o deterioramento di habitat all'interno di un sito protetto; impiego di cittadini di paesi terzi irregolari; favoreggiamento della permanenza illegale dello straniero; dichiarazione ai fini delle imposte dirette o dell'IVA fraudolenta per uso di fatture false oggettivamente o soggettivamente, per altri artifici o altrimenti infedele; occultamento o distruzione dei documenti contabili; compensazione indebita ai danni dell'UE; sottrazione fraudolenta al pagamento di imposte; falsificazione in scrittura privata relativa a beni culturali; esportazione illecita di beni culturali; distruzione di beni culturali; riciclaggio di beni culturali	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (art. 491-bis c.p.);** **Art. 25 d.lgs. 231/2001 (artt. 314, 314-bis, 316, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25 ter d.lgs 231/2001 (art. 2635, 2635-bis c.c.);** **Art. 25-septies d.lgs 231/2001;** **Art. 25-octies d.lgs. 231/2001 (artt. 648-bis, 648-ter c.p.)** **L. 190/2012 (art. 328 c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 356, 640, 640-bis, 640-ter, c.p.);** **Art. 25-ter d.lgs 231/2001 (art. 2635, 2635-bis c.c.);** **Art. 25-undecies d.lgs 231/2001 (art. 452 bis, 452 quater, 452 quinquies, 733-bis c.p.);** **Art. 25-duodecies d.lgs 231/2001;** **Art. 25-quinquiesdecies d.lgs. 231/2001 (art. 2,3, 4, 5, 10, 10-quater, 11 d.lgs. 74/2000);** **Art. 25-septiesdecies d.lgs. 231/2001 (artt. 518-octies, 518-undecies; 518-duodecies c.p.);** **Art. 25-duodevicies d.lgs. 231/2001 (art. 518-sexies, c.p.)**

V.5.2. ATTIVITÀ A RISCHIO E POTENZIALI REATI (BUSINESS DEVELOPMENT)

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001

Promozione delle attività di cessione dei diritti d'uso su fibra ottica e fornitura di servizi accessori	Resp. funzione, Soggetti legittimati	Truffa in danno dello Stato o di altro ente pubblico o dell'UE; frode nelle pubbliche forniture; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; concussione, corruzione attiva e passiva, istigazione alla corruzione, traffico di influenze illecite	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (art. 640 c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 356, 640-bis, 640-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 317, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.)**
Definizione dei contratti per la cessione di diritti d'uso su fibra ottica e per la fornitura di servizi accessori	Resp. funzione, Soggetti legittimati	Concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione tra privati; istigazione alla corruzione tra privati; frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE	**RISCHIO DIRETTO:** **Art. 25 d.lgs. 231/2001 (artt. 317, 318, 319, 319-bis, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis c.c.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 356, 640, 640-bis, 640-ter c.p.)**
Monitoraggio del rispetto degli SLA contrattuali e dell'incasso dei corrispettivi relativi alla cessione delle infrastrutture e dei servizi accessori	Resp. funzione, CDG	Danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione tra privati; istigazione alla corruzione tra privati; frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE	**RISCHIO DIRETTO:** **Art. 24-bis (artt. 635-bis, 635-ter c.p.);** **Art. 25 d.lgs. 231/2001 (artt. 317, 318, 319, 319-bis, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis c.c.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 356, 640, 640-bis, 640-ter c.p.)**
Predisposizione e monitoraggio delle convenzioni per la gestione e manutenzione di reti regionali	Resp. funzione	Concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE	**RISCHIO DIRETTO:** **Art. 25 d.lgs. 231/2001 (artt. 317, 318, 319, 319-bis, 319-quater, 320, 321, 322, 346-bis, c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 356, 640, 640-bis, 640-ter c.p.)**
Monitoraggio delle attività di regolamentazione del mercato di riferimento, della gestione delle relazioni con i clienti e le associazioni di categoria del comparto per la valutazione delle offerte commerciali	Resp. funzione	Accesso abusivo a sistema informatico o telematico; frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (art. 615-ter c.p.);** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (Artt. 356, 640, 640-bis, 640-ter c.p.)**

V.5.3. ELEMENTI DI CONTROLLO PER BUSINESS DEVELOPMENT

Per il complesso di attività svolte dall'Ufficio Business Development, Infratel Italia assicura che l'individuazione delle opportunità di business ed il successivo sviluppo siano coerenti con la mission aziendale e con gli obiettivi strategici definiti dai vertici aziendali.

Le attività di scouting, finalizzate all'individuazione di possibili opportunità commerciali, ovvero le attività di negoziazione con il committente, finalizzate alla definizione dei contenuti e degli aspetti tecnici, operativi ed economici degli accordi/convenzioni, sono condotte dall' Amministratore Delegato, in collaborazione con gli Uffici interni preposti e competenti, nel rispetto dei codici di condotta e dei protocolli di gestione relativi alle modalità di rapporto con soggetti della Pubblica Amministrazione.

il Direttore Generale e il Responsabile Business Development assicurano che l'individuazione delle opportunità commerciali sia coerente con la mission e con gli obiettivi strategici aziendali.

Possono intrattenere rapporti di natura commerciale con terze parti di natura privata per conto di Infratel Italia solamente i soggetti (dipendenti, membri degli organi sociali, collaboratori esterni, consulenti o partner) **a cui è stato formalmente conferito incarico in tal senso** (con apposita procura o disposizione organizzativa per i soggetti interni, ovvero con apposita clausola nel contratto di collaborazione o consulenza o partnership per gli altri soggetti indicati).
Gli incontri con i rappresentanti di detti enti, quali meeting di natura decisionale o programmatica, strumentali o finalizzati alla formalizzazione di contratti/accordi/convenzioni, devono essere presenziati preferibilmente almeno da due rappresentanti della Società: comunque di detti incontri deve essere tenuta traccia della data, degli obiettivi/motivazioni, dei partecipanti e dell'esito degli stessi. Tali informazioni dovranno essere comunicate al proprio responsabile ed al RPCT[57], quindi archiviate e conservate dalla segreteria di riferimento.
Gli incontri devono essere condotti nel rispetto delle regole comportamentali espresse nel Codice Etico e sinteticamente richiamati nei punti che seguono:

- non è consentito a coloro che operano per conto di Infratel Italia, né direttamente né indirettamente o per il tramite di interposta persona, realizzare attività, sotto qualsiasi forma, che abbiano come effetto l'illecito condizionamento di soggetti terzi anche di natura privata quali operatori, fornitori o partner della Società. Pertanto, non è consentito offrire o promettere denaro, doni, compensi, o altra utilità sotto qualsiasi forma, né esercitare illecite pressioni ovvero dare o promettere beni, servizi, prestazioni, favori o altre utilità a dirigenti, funzionari o dipendenti di detti enti, o a loro parenti o conviventi, anche per il tramite di interposta persona, allo scopo di influenzare il loro giudizio nell'ambito di qualsiasi tipologia di rapporto con gli stessi instaurato;
- è fatto obbligo di instaurare e gestire qualsiasi rapporto con soggetti terzi, quali operatori, fornitori o partner, secondo criteri di massima correttezza, imparzialità, trasparenza e buona fede. Non è consentito utilizzare o presentare dichiarazioni o documenti attestanti fatti e notizie non vere ovvero omettere informazioni per conseguire, a vantaggio o nell'interesse di Infratel Italia, qualsiasi beneficio di natura commerciale.

Chiunque riceva richieste, esplicite o implicite, di benefici, favori o utilità di qualsiasi natura da parte di dirigenti, funzionari o dipendenti di un ente terzo privato, ovvero sia indotto dagli stessi a dare o promettere denaro o altre utilità, è tenuto ad informare tempestivamente l'Organismo di Vigilanza e il RPCT e a sospendere immediatamente ogni rapporto con essi.
Qualora Infratel Italia faccia ricorso a partner commerciali o consulenti esterni, questi sono tenuti al rispetto dei principi e delle regole di gestione espresse nel presente documento anche attraverso la previsione, nell'ambito dei contratti di partnership o collaborazione, di specifiche clausole di risoluzione in caso di violazione di dette regole nonché di quelle contenute nel Codice Etico.
La selezione di eventuali partner commerciali è effettuata sulla base di criteri oggettivi, trasparenti e documentati; in particolare, **in caso di nuove opportunità di non riconosciuta attendibilità, l'Ufficio Business Development effettua le opportune verifiche in linea con quanto previsto in tema di affidabilità e onorabilità dei fornitori**.
Qualora sia necessario prevedere le condizioni tecnico-economiche relative alla vendita di servizi e agli eventuali accordi di partnership, queste sono predisposte dall'Ufficio Business Development in collaborazione con le funzioni tecniche competenti per la valutazione degli interventi e dei costi necessari. Le condizioni di offerta[58] sono determinate in base a corrispettivi prestabiliti nell'ambito dei contratti/convenzioni stipulate con il committente.
Gli accordi formali che Infratel Italia stipula con operatori o eventuali partner sono elaborati dall'Ufficio Business Development in collaborazione con l'Ufficio Affari Legali presso la Capogruppo, quindi sottoposti a validazione e firma da parte dei Soggetti titolati[59], in base ai poteri di firma. In tali accordi deve essere presente un'apposita

[57] Secondo le tempistiche dallo stesso definite. Le motivazioni di eventuali deroghe alla predisposizione della sintesi degli incontri sono oggetto di comunicazione tempestiva al RPCT.
[58] L'Ufficio è tenuto a mantenere traccia tutte le richieste di cessione ricevute
[59] In base ai poteri conferiti dal sistema di procure e deleghe in essere. I soggetti firmatari sono tenuti a sottoscrivere un'attestazione

clausola risolutiva che regoli il caso di commissione da parte della controparte contrattuale di fatti rilevanti ai sensi del D.Lgs. 231/01 o di violazione delle regole stabilite dal Modello 231, Parte Generale e Parte Speciale, e dal Codice Etico di Infratel Italia.

Nell'ambito di ciascun accordo è identificato un Referente interno/Responsabile di Progetto, responsabile della corretta prestazione/fornitura, nel rispetto dei requisiti formalizzati; tale soggetto è tenuto a documentare/certificare l'avvenuta prestazione/fornitura e le relative modalità di erogazione, anche sulla base di quanto previsto dal rapporto contrattuale, oggetto di verifica e approvazione da parte dell'area Gestione Rete.

I Corrispettivi relativi alla cessione delle infrastrutture si riferiscono alle seguenti voci: l'IRU cioè il diritto d'uso (per le PA è gratuito); il servizio accessorio di manutenzione; eventuali costi di set-up o di attivazione.

Per quanto riguarda l'incasso dei corrispettivi, l'Ufficio riceve dall'Amministrazione eventuali segnalazioni di fatture non pagate e procede ad un primo sollecito informale con l'operatore. Se tale sollecito resta inascoltato, la pratica passa alla competenza dell'Ufficio Controllo di Gestione.

L'Ufficio effettua le valorizzazioni attraverso delle procedure operative standard e listini ufficiali. Nel caso di servizi nuovi o necessità di mutare i prezzi, e al contempo per formulare offerte che rispondano ai parametri predefiniti, richiede il supporto di AGCOM o del CDA, affinché approvino un nuovo listino.

L'Ufficio si occupa anche del controllo del rispetto degli SLA dal lato dell'operatore e della gestione di eventuali reclami per mancato rispetto delle tempistiche imputabili ad Infratel Italia e dell'inoltro dei reclami agli Uffici di competenza.

La fattura attiva viene predisposta dal *Service* Amministrazione e Bilancio sulla base dell'avvenuto inserimento a sistema delle necessarie informazioni da parte dell'Ufficio Gestione Reti, il quale è tenuto anche alla verifica di corrispondenza tra ordine/contratto di vendita ed effettiva esecuzione della prestazione/fornitura, previo benestare formale da parte del Referente interno (o Responsabile di Progetto).

L'emissione della fattura inerente a una penale o una rivalsa costi per inadempienza di soggetti terzi viene predisposta da Amministrazione e Bilancio sulla base delle informazioni ricevute dalle funzioni interne competenti previa autorizzazione formale da parte dei Soggetti titolati della Società.

Le fatture, sia attive che inerenti a penali, sono inviate formalmente tramite PEC a cura dell'Amministratore Delegato o responsabili incaricati.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate, l'Ufficio Business Development è tenuto alla comunicazione periodica, su base annuale, all'Organismo di Vigilanza ed al RPCT di un'informativa riepilogativa dei nuovi contratti/accordi/convenzioni sottoscritti e di una tempestiva comunicazione per adempiere agli obblighi relativi alla normativa sulla "trasparenza".

In ogni caso, il responsabile dell'Ufficio Business Development comunica all'OdV e al RPCT, con cadenza almeno annuale, le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

V.5.4. ULTERIORI ELEMENTI DI CONTROLLO PER BUSINESS DEVELOPMENT

Tra le responsabilità dell'unità organizzativa Business Development vi è quella dell'analisi della Proposta di modelli di business finalizzati allo sviluppo del "Sistema informativo nazionale federato delle infrastrutture" (S.I.N.F.I.).

Nella mappatura dei rischi tale attività risulta meramente strumentale, in quanto consiste in attività di sviluppo priva di un significativo margine di esposizione. Tuttavia, non si può escludere che una grave carenza del suo svolgimento possa agevolare od occultare la commissione di un illecito, né, altresì, può escludersi che i responsabili di tale funzione partecipino in concorso con le funzioni coinvolte in altre ipotesi di rischio, divenendo in tal caso essi stessi direttamente autori dell'illecito.

del rispetto delle regole definite nel Modello 231, Parte Generale e Parte Speciale ex D.Lgs. 231/01 e nel PPCT ex L. 190/12 e del Codice Etico

Di seguito il riepilogo delle attività meramente strumentali:

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Proposta di modelli di business finalizzati allo sviluppo del "Sistema informativo nazionale federato delle infrastrutture" (S.I.N.F.I.)	Resp. funzione	frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE	**RISCHIO STRUMENTALE: Art. 24 d.lgs 231/2001 (artt. 356, 640, 640-bis, 640-ter c.p.)**

Al fine di prevenire gli ulteriori rischi di illecito correlati a questa attività meramente strumentale, il *risk owner* di primo livello svolge la propria attività in coordinamento con le altre funzioni interne e della Capogruppo coinvolte, rispettando i principi generali di controllo e il codice etico, avendo come punti di attenzione i rischi strumentali sopra indicati.
Il *process owner* garantisce l'effettività e l'efficacia dei controlli, effettuando la sorveglianza sul loro corretto svolgimento ed a tal fine richiede una informativa ai *risk owner,* sulla base della quale egli acquisisce le informazioni rilevanti al fine di alimentare i flussi verso l'OdV.

V.5.5. ATTIVITÀ A RISCHIO E POTENZIALI REATI (GESTIONE SINFI)

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001
Gestione sistema SINFI	Resp. funzione	Indebita percezione di erogazioni pubbliche; truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; falsità in documento pubblico informatico; accesso abusivo a sistema informatico o telematico; intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche; detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; danneggiamento di sistemi informatici o telematici; detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico; danneggiamento di sistemi informatici o telematici di pubblico interesse; malversazioni di erogazioni pubbliche; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione tra privati; istigazione alla corruzione tra privati; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza	**RISCHIO DIRETTO: Art. 24 d.lgs 231/2001 (artt. 316-ter, 640, 640-bis, 640-ter c.p.); Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater, 635-quater.1, 635-quinquies c.p.)** **RISCHIO STRUMENTALE: Art. 24 d.lgs 231/2001 (art. 316-bis c.p.); Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 317, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.); Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis, 2638 c.c.)**

V.5.6. ATTIVITÀ A RISCHIO E POTENZIALI REATI (GESTIONE RETE)

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001

Progettazione e gestione della Rete di Backhauling	Resp. funzione	Truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; falsità in documento pubblico informatico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale; messa a disposizione del pubblico di un'opera dell'ingegno protetta o di parte di essa; duplicazione abusiva di programmi per elaboratore; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori; riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati; abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere scientifiche; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa; omessa segnalazione alla Autorità giudiziaria o alla P.G. di condotte penalmente rilevanti ai sensi della L. n. 633/1941, degli artt. 615-ter e 640-ter c.p.; Omessa comunicazione all'AGCOM un punto di contatto diretto; malversazione di erogazioni pubbliche; Indebita percezione di erogazioni pubbliche; frode nelle pubbliche forniture; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; turbata libertà dell'industria o del commercio; illecita concorrenza con minaccia o violenza; corruzione tra privati; istigazione alla corruzione tra privati	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (artt. 640, 640-bis, 640-ter c.p.);** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 635-bis, 635-ter c.p.);** **Art. 25-bis.1 (art. 517-ter c.p.);** **Art. 25-novies d.lgs 231/2001 (artt. 171, 171-bis, 171-ter, 174-sexies L. n. 633/1941)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 356 c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 317, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25-bis.1 d.lgs 231/2001 (artt. 513, 513-bis, 517-ter c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis c.c.)**
Esecuzione degli interventi diretti previsti dai Piani tecnici	Resp. funzione	Malversazione di erogazioni pubbliche; frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; omicidio colposo e lesioni gravi o gravissime colpose - commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro; inquinamento ambientale; delitti colposi contro l'ambiente; distruzione o deterioramento di habitat all´interno di un sito protetto; falsificazione in scrittura privata relativa a beni culturali; uscita o esportazione illecite di beni culturali; distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici; riciclaggio di beni culturali; impiego di cittadini di paesi terzi il cui soggiorno è irregolare	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 356, 640, 640-bis, 640-ter c.p.);** **Art. 25-septies d.lgs 231/2001;** **Art. 25-undecies d-lgs 231/2001 (artt. 452-bis. 452-quinquies, 733-bis c.p.);** **Art. 25-septiesdecies d.lgs. 231/2001 (artt. 518-octies, 518-undecies; 518-duodecies c.p.);** **Art. 25-duodevicies d.lgs. 231/2001 (art. 518-sexies, c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 356, 640, 640-bis, 640-ter c.p.);** **Art. 25-duodecies (art. 22 comma 12-bis, d.lgs n. 286/1998)**

Manutenzione e delivery dei servizi ai clienti della Rete diretta in gestione.	Resp. funzione	Peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; omicidio colposo e lesioni gravi o gravissime colpose - commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro; malversazione di erogazioni pubbliche; frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; falsità in documento pubblico informatico; accesso abusivo a sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; corruzione tra privati; istigazione alla corruzione tra privati; impiego di cittadini di paesi terzi il cui soggiorno è irregolare; falsificazione in scrittura privata relativa a beni culturali; uscita o esportazione illecite di beni culturali; distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici; riciclaggio di beni culturali	**RISCHIO DIRETTO:** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 317, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25-septies d.lgs 231/2001** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 356, 640, 640-bis, 640-ter c.p.);** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.);** **Art. 25-ter d.lgs 231/2001 (art. 2635, 2635-bis c.c.);** **Art. 25-duodecies (art. 22 comma 12-bis d.lgs n. 286/1998);** **Art. 25-septiesdecies d.lgs. 231/2001 (artt. 518-octies, 518-undecies; 518-duodecies c.p.);** **Art. 25-duodevicies d.lgs 231/2001 (art. 518-sexies, c.p.)**
Gestione delle procedure per l'ottenimento dei permessi e delle autorizzazioni in materia di conformità ambientale, paesaggistica, territoriale e urbanistica	Resp. funzione/A.D./ D.G./delegato	Falsità in documento pubblico informatico; accesso abusivo a sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; turbata libertà degli incanti; turbata libertà del procedimento di scelta del contraente; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; inquinamento ambientale; delitti colposi contro l'ambiente; distruzione o deterioramento di habitat all´interno di un sito protetto; falsificazione in scrittura privata relativa a beni culturali; uscita o esportazione illecite di beni culturali; distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici; riciclaggio di beni culturali	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 317, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis 316-ter, 353, 353-bis, 640, 640-bis, 640-ter c.p.);** **Art. 25-ter d.lgs 231/2001 (art. 2638 c.c.);** **Art. 25-undecies (artt. 452-bis, 452-quinquies, 733-bis c.p.);** **Art. 25-septiesdecies d.lgs. 231/2001 (artt. 518-octies, 518-undecies; 518-duodecies c.p.);** **Art. 25-duodevicies d.lgs. 231/2001 (art. 518-sexies, c.p.)**
Gestione del processo di acquisizione di infrastrutture e assunzione del ruolo di RUP	Resp. funzione/RUP	malversazione di erogazioni pubbliche; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione tra privati; istigazione alla corruzione tra privati; rifiuto d'atti d'ufficio. omissione ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (art. 491-bis c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 317, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (art. 2635, 2635-bis c.c.)** **Art. 25-septies d.lgs 231/2001;** **Art. 25-octies d.lgs 231/2001;** **Art. 25-undecies d.lgs 231/2001 (artt. 452-bis, 452-quater, 452-quinquies, 452-octies, 733-bis c.p.);** **Art. 25-septiesdecies d.lgs 231/2001 (artt. 518-octies, 518-undecies; 518-duodecies c.p.);** **Art. 25-duodevicies d.lgs 231/2001 (art. 518-sexies c.p.)**

			L. 190/2012 (art. 328 c.p.) **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 356, 640, 640-bis, 640-ter c.p.);** **Art. 25 duodecies (artt. 12, commi 3, 3-bis, 3-ter e 5, e art. 22, comma 12-bis, d.lgs. 286/1998);** **Art. 25-quinquiesdecies d.lgs 231/2001 (art. 2, 3, 8, 10, 11 d.lgs. 74/2000);**
Monitoraggio e supervisione della rete a favore del Ministero competente e delle regioni	Resp. funzione	Falsità in documento pubblico informatico; accesso abusivo a sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; indebita percezione di erogazioni pubbliche; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; corruzione tra privati; istigazione alla corruzione tra privati; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza; inquinamento ambientale; delitti colposi contro l'ambiente; distruzione o deterioramento di habitat all'interno di un sito protetto	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001(artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.);** **Art. 25 d.lgs. 231/2001 (artt. 317, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-ter, 640, 640-bis, 640-ter c.p.);** **Art. 24-bis d.lgs 231/2001 (artt.491-bis, 615-ter, 635-bis, 635-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316 c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis, 2638 c.c.);** **Art. 25-undecies d.lgs 231/2001 (artt. 452-bis, 452-quinquies, 733-bis c.p.)**
Gestione della documentazione di rete nel Network Inventory della rete di Backhauling e di accesso	Resp. funzione	Truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; falsità in documento pubblico informatico; accesso abusivo a sistema informatico o telematico; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (artt. 640, 640-bis, 640-ter c.p.);** **Art. 24-bis d.lgs 231/2001 (artt. 491-bis, 615-ter, 635-bis, 635-ter c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316 c.p.);** **Art. 25-ter d.lgs 231/2001 (art. 2638 c.c.)**

V.5.7. ATTIVITÀ A RISCHIO E POTENZIALI REATI (AREE OPERATIONS)

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001

Coordinamento delle attività relative agli interventi infrastrutturali attuati da Infratel nell'ambito territoriale di competenza (Piano Italia 1 Giga e Concessione)	Resp. area, Resp. IO	Malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione e istigazione alla corruzione tra privati	**RISCHIO DIRETTO:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 316-ter, 356, 640, 640-bis, 640-ter c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 317, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (artt. 2635, 2635-bis c.c.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 356, 640, 640-bis, 640-ter c.p.);** **Art. 25 d.lgs. 231/2001 (artt. 314, 314-bis, 316, 317, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.)**
RUP per l'esecuzione dei relativi contratti	Resp. area, Resp. IO	Falsità in documento pubblico informatico; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; rifiuto d'atti d'ufficio. omissione malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita; autoriciclaggio; dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti; dichiarazione fraudolenta mediante altri artifici; emissione di fatture o altri documenti per operazioni inesistenti; occultamento o distruzione di documenti contabili; sottrazione fraudolenta al pagamento di imposte	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (art. 491-bis c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 317, 318, 319, 319-quater, 320, 321, 322, 346-bis, c.p.)** **L. 190/2012 (art. 328 c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 356, 640, 640-bis, 640-ter c.p.);** **Art. 25-octies d.lgs 231/2001;** **Art. 25-quinquiesdecies d.lgs 231/2001 (art. 2, 3, 8, 10, 11 d.lgs 74/2000)**

V.5.8. ATTIVITÀ A RISCHIO E POTENZIALI REATI (PIANO ISOLE MINORI)

ATTIVITÀ' SENSIBILI	SOGGETTI	CONDOTTA ILLECITA	Fattispecie ex d.lgs. 231/2001

Ambito ISOLE MINORI: assicura l'esecuzione dell'attività definita dal relativo Piano Operativo	Resp. area, Resp. IO	Falsità in documento pubblico informatico; peculato, peculato mediante profitto dell'errore altrui, indebita destinazione di denaro o cose mobili - quando i fatti offendono gli interessi finanziari dell'UE; concussione; corruzione attiva e passiva; induzione indebita a dare o promettere utilità; istigazione alla corruzione; traffico di influenze illecite; corruzione e istigazione alla corruzione tra privati; rifiuto d'atti d'ufficio. omissione malversazione di erogazioni pubbliche; indebita percezione di erogazioni pubbliche; frode nelle pubbliche forniture; truffa in danno dello Stato o di altro ente pubblico o dell'UE; truffa aggravata per il conseguimento di erogazioni pubbliche; frode informatica in danno dello Stato o di altro ente pubblico o dell'UE; omicidio colposo e lesioni gravi o gravissime colpose - commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro; ricettazione; riciclaggio; impiego di denaro, beni o utilità di provenienza illecita; autoriciclaggio; inquinamento ambientale; disastro ambientale; delitti colposi contro l'ambiente; distruzione o deterioramento di habitat all'interno di un sito protetto; condotte favorenti l'immigrazione clandestina; impiego di cittadini di paesi terzi il cui soggiorno è irregolare; dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti; dichiarazione fraudolenta mediante altri artifici; emissione di fatture o altri documenti per operazioni inesistenti; occultamento o distruzione di documenti contabili; sottrazione fraudolenta al pagamento di imposte; falsificazione in scrittura privata relativa a beni culturali; uscita o esportazione illecite di beni culturali; distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici; riciclaggio di beni culturali	**RISCHIO DIRETTO:** **Art. 24-bis d.lgs 231/2001 (art. 491-bis c.p.);** **Art. 25 d.lgs 231/2001 (artt. 314, 314-bis, 316, 317, 318, 319, 319-quater, 320, 321, 322, 346-bis c.p.);** **Art. 25-ter d.lgs 231/2001 (art. 2635, 2635-bis c.c.)** **Art. 25-septies d.lgs 231/2001;** **Art. 25-octies d.lgs 231/2001;** **Art. 25-undecies d.lgs 231/2001 (artt. 452-bis, 452-quater, 452-quinquies, 452-octies, 733-bis c.p.);** **Art. 25-septiesdecies d.lgs 231/2001 (artt. 518-octies, 518-undecies; 518-duodecies c.p.);** **Art. 25-duodevicies d.lgs 231/2001 (art. 518-sexies c.p.)** **L. 190/2012 (art. 328 c.p.)** **RISCHIO STRUMENTALE:** **Art. 24 d.lgs 231/2001 (artt. 316-bis, 356, 640, 640-bis, 640-ter c.p.);** **Art. 25 duodecies (artt. 12, commi 3, 3-bis, 3-ter e 5, e art. 22, comma 12-bis, d.lgs. 286/1998);** **Art. 25-quinquiesdecies d.lgs 231/2001 (art. 2, 3, 8, 10, 11 d.lgs. 74/2000);**

V.5.9. ELEMENTI DI CONTROLLO PER GESTIONE RETE, AREE OPERATIONS, FUNZIONE DI RUP E PIANI OPERATIVI CONCESSIONE E 1 GIGA

Le attività delle aree **a rischio Infrastrutture e Operations** e i relativi elementi di controllo si riferiscono a tutte le unità organizzative (Gestione Rete, Gestione SINFI, Aree Operations Nord Ovest, Nord Est, Centro, Sud, Isole) cui compete la realizzazione degli interventi mediante affidamento diretto, concessione (operations concessione) e incentivo (Piano Italia 1 Giga).

Le attività sensibili sono state identificate per singolo Ufficio e gli elementi di controllo sono comuni a tutti gli Uffici che compongono l'Area a rischio Infrastrutture e Operations.

Infratel Italia assicura che le attività di progettazione e realizzazione delle infrastrutture di rete siano condotte in maniera corretta, trasparente e tracciabile, nel rispetto delle condizioni previste dal contratto/convenzione stipulati con il committente e della normativa vigente e applicabile alla Società.

Il Responsabile dell'Ufficio Gestione Rete, il Responsabile dell'Ufficio Infrastrutture e Operations o il Responsabile delle aree Operations, (in seguito anche indicati indistintamente come Responsabile Ufficio, ruolo svolto da tutti e tre in relazione alla propria sfera di competenza) propongono l'organigramma di commessa/progetto, nel quale sono indicati il Responsabile di commessa/RUP oltre agli altri adempimenti previsti specificamente dalla normativa sui contratti pubblici ivi inclusa la dichiarazione sul conflitto di interessi, nonché tutte le risorse costituenti il team di commessa/progetto e lo sottopongono per approvazione all'Amministratore delegato. L'Ufficio Risorse Umane provvede a comunicare l'organigramma, approvato dall'Amministratore delegato, a tutti i soggetti/Uffici interessati, attraverso la pubblicazione sulla intranet aziendale.

Infratel Italia assicura la regolare esecuzione delle attività svolte (attività di commessa o progetto), nel rispetto di quanto previsto nel contratto/convenzione e nel Piano associato.

Gli Uffici dell'area Infrastrutture e Operations supportano e collaborano con i Responsabili di commessa/progetto, opportunamente identificati e nominati dall'Amministratore Delegato[60], nelle attività di sviluppo e nel monitoraggio di tempi e costi di ciascuna commessa o progetto.

Gli Uffici dell'area Infrastrutture e Operations, ciascuno per gli interventi di propria competenza, **elaborano il Piano Operativo contenente i parametri tecnici ed economici di dettaglio della commessa/progetto/piano**.

Le commesse/progetti sono scandite per fasi da suddividersi in: apertura commessa; programmazione e avvio; gestione e controlli; rendicontazione; chiusura commessa. L'ufficio, nelle fasi preliminari, si coordina con l'unità Pianificazione, Gare e Ingegneria per definire l'accordo di programma/convenzione con Infratel Italia o con le Regioni e il relativo piano operativo per gli adempimenti di gara.

Il RUP per la convenzione è scelto tra i responsabili degli uffici coinvolti, nel rispetto delle misure organizzative e dei requisiti di legge, conformemente a quanto previsto per l'unità Pianificazione, Gare e Ingegneria, al paragrafo "Svolgimento del ruolo di RUP per tutti i procedimenti di affidamento per il rispetto degli adempimenti normativi e del sistema di e-procurement".

Il RUP per l'esecuzione è generalmente scelto tra le aree operations interessate.

Il Responsabile di commessa/RUP in collaborazione con la funzione Affari Legali di Capogruppo, a quella interna Legale e Controllo Operativo PNRR, per quanto di competenza con Verifiche cantieri, anche per le opportune verifiche di qualità e SSL, è tenuto a monitorare il rispetto del Piano operativo, comunicando eventuali varianti, scostamenti o anomalie all'Ufficio competente per la definizione di opportune azioni, da comunicare, se necessario, all'Ufficio Pianificazione Gare e Ingegneria.

Il Responsabile di commessa/RUP assicura, nel rispetto del Piano operativo, la realizzazione (nel caso di affidamenti diretti o incentivi) o l'acquisizione dal concessionario (nel caso di concessioni) della progettazione preliminare/definitiva/esecutiva, corredata dei documenti previsti dalla norma di riferimento, e la sottopone al Responsabile dell'Ufficio per l'approvazione. Comunica formalmente all'appaltatore l'avvenuta approvazione della progettazione. Il Responsabile di Commessa/RUP deve inoltre monitorare, evidenziando al Responsabile dell'Ufficio eventuali scostamenti, il rispetto dei tempi previsti dai contratti di appalto, di concessione e a incentivo.

Con specifico riferimento al modello "incentivo", durante le fasi di esecuzione lavori sono svolte le verifiche tecniche in merito allo stato delle attività tramite report di avanzamento, trasmessi dal beneficiario, e eventuali sopralluoghi, per mezzo di un verbale di sopralluogo sul cantiere effettuati dal personale Infratel Italia, e formalizzati attraverso la compilazione di opportuna documentazione preliminarmente predisposta. I controlli possono essere svolti mediante verifiche *in situ* a campione e/o tramite video ispezioni da remoto, nonché mediante altri controlli tecnici adeguati in termini di affidabilità, con altri mezzi tecnologici. I report sono tracciati tramite il sistema informativo di gestione commesse o altro strumento equivalente con i dati relativi all'avanzamento delle attività. Deve inoltre essere garantita segregazione funzionale tra chi contribuisce all'elaborazione della documentazione di supporto alle attività di monitoraggio e controllo e chi svolge le attività di attuazione e gestione.

Con specifico riferimento al modello "diretto", il Responsabile di commessa/RUP, durante tutte le fasi della commessa, verifica costantemente l'eventuale esistenza di infrastrutture di proprietà di operatori o altri

[60] Sulla base di criteri prestabiliti tra cui esperienza, competenza e ottimizzazione logistica.

enti/società territoriali per minimizzare le attività di scavo e procedere al riuso di tutta l'infrastruttura esistente. Qualora siano rilevate infrastrutture non precedentemente acquisite e idonee all'utilizzo, il Responsabile Gestione Rete valuta la possibilità di stipulare un contratto per l'acquisizione dei diritti d'uso della rete[61]. Le stesse valutazioni vanno ponderate anche per minimizzare l'impatto in termini ambientali e per evitare che le operazioni di scavo comportino danni o pericoli per beni culturali eventualmente presenti nel sottosuolo o lungo il tracciato.

Il Responsabile di Commessa/RUP è tenuto alla formalizzazione del **contratto attuativo[62]** avente ad oggetto la realizzazione dell'intervento nell'ambito del modello diretto, assicurandone la coerenza con la progettazione esecutiva e con l'accordo quadro di riferimento. Il contratto attuativo è verificato dall'Ufficio Gestione Rete ed approvato dall'Amministratore Delegato, dagli altri soggetti titolati e/o dal Consiglio di Amministrazione, in funzione dell'importo e dei limiti di spesa previsti dal sistema di procure e deleghe vigente. È fatto divieto di dare esecuzione alle attività senza che si sia preventivamente proceduto alla sottoscrizione dell'accordo formale tra le parti.

Nel modello diretto, il Responsabile di Commessa/RUP è tenuto, a fronte di una richiesta di autorizzazione al sub-appalto, alla verifica di correttezza e completezza della documentazione ricevuta ed alla formalizzazione degli esiti di tale verifica. Solo in seguito all'esito positivo della verifica, il sub-appalto potrà essere autorizzato, dandone comunicazione all'appaltatore richiedente a cura del Responsabile Unico del Progetto. Le verifiche devono riguardare anche il rispetto della sicurezza del cantiere, la gestione ambientale, paesaggistica, la tutela dei beni archeologici e ogni altro aspetto ricadente tra le prerogative del Responsabile Unico del Progetto, in base alla normativa sui contratti pubblici.

Il Direttore Lavori (nominato dall'Amministratore Delegato o da altro soggetto titolato[63] su proposta del Responsabile Gestione Rete, nel caso degli interventi in affidamento diretto, e nominato dal Concessionario nel caso di interventi in concessione) assicura e certifica la corretta esecuzione dei lavori nel rispetto del progetto esecutivo e delle specifiche di realizzazione predefinite, attraverso la predisposizione di documenti attestanti lo stato di avanzamento dei lavori.

Sempre con riferimento al modello diretto, esegue anche il collaudo delle opere, oggetto di approvazione formale da parte del RUP, scelto tra i Responsabili degli uffici interessati, nel rispetto dei principi di competenza, rotazione, dell'assenza di conflitto di interessi e degli altri requisiti di legge (v. paragrafo "Gestione Gare" in Pianificazione, Gare e Ingegneria).

Nei casi di affidamenti diretti, in cui la scelta del Direttore Lavori è di competenza di Infratel Italia, la selezione del Direttore Lavori a cui assegnare l'incarico avviene nel rispetto di specifici criteri[64], predefiniti dall'Ufficio interessato ed oggetto di approvazione da parte dell'Amministratore Delegato o dagli altri soggetti titolati in base al sistema di procure e deleghe. Eventuali ritardi, anomalie o non conformità rilevate dal Direttore Lavori nello svolgimento delle suddette attività, corredate dalle azioni correttive/risolutive stabilite, sono comunicate al Responsabile di Commessa/RUP e sottoposte ad autorizzazione da parte del Responsabile dell'Ufficio interessato. Per il modello a concessione, invece, i collaudi vengono eseguiti da personale interno dell'area Operations o da risorse esterne.

Nell'esecuzione e nello sviluppo degli interventi diretti previsti nei Piani tecnici l'Ufficio Gestione Rete supervisiona l'operato dei lavori, insieme al Direttore Lavori. Dopo l'avvio dei lavori, l'Ufficio si occupa del

[61] Nel rispetto degli elementi di controllo stabiliti per il processo di ciclo passivo

[62] Nel rispetto degli elementi di controllo stabiliti per il processo di ciclo passivo

[63] Sulla base del sistema di procure e deleghe

[64] In ordine a ragioni di esperienza, competenza ed in relazione alla necessità di adottare criteri di rotazione

monitoraggio, che si sostanzia nel: rispetto del cronoprogramma; monitoraggio tramite applicazioni (Geo4wip) in merito allo SLA (Service Level Agreement); controllo dei SAL per la componente economica; controllo puntuale e continuo del Direttore Lavori, presente sul cantiere.

Sono predisposte delle checklist per la verifica puntuale della completezza della documentazione, delle autorizzazioni e degli altri adempimenti formali che l'impresa appaltatrice deve rispettare nel corso dei lavori.

Con riferimento al modello diretto e al modello a concessione, il Responsabile di commessa/RUP è tenuto a monitorare il rispetto del Piano associato al contratto e al Piano operativo di progetto, comunicando eventuali varianti, scostamenti o anomalie al Responsabile Gestione Rete per la definizione di opportune azioni oggetto di condivisione, se necessario, con l'Ufficio Business Development o Pianificazione, Gare e Ingegneria. In particolare, eventuali varianti in corso d'opera, da gestire in accordo al Codice degli Appalti e/o al contratto/convenzione di riferimento, sono proposte dal Direttore Lavori quindi verificate dal Responsabile di commessa/RUP e sottoposte ad autorizzazione da parte del Responsabile Gestione Rete e dei Soggetti titolati della Società in accordo al sistema di procure e deleghe vigente; quindi, comunicate[65] agli enti preposti nei termini stabiliti dalla normativa applicabile.

Il Responsabile di Commessa/RUP, con il supporto dell'Ufficio Rendicontazione, assicura, sulla base delle scadenze previste dal contratto/convenzione, l'attuazione delle attività preordinate al processo di rendicontazione verso il committente nel rispetto dei codici di condotta e degli elementi di controllo relativi al processo di Rendicontazione stabiliti nel presente documento.

Le attività di monitoraggio della commessa/progetto sono svolte periodicamente dall'Ufficio competente.

Qualora si verifichi un evento straordinario in grado di incidere sul budget complessivo di commessa/progetto e di conseguenza sul Piano operativo, il Responsabile di commessa/progetto valuta di concerto con l'Ufficio competente, informando l'Amministratore Delegato, se coinvolgere i comitati di controllo preposti, ove esistenti, chiamati a sovraintendere il monitoraggio della commessa.

Il Responsabile di Commessa/RUP, con il supporto di Rendicontazione, assicura, sulla base delle scadenze previste dal contratto/convenzione, l'attuazione delle attività preordinate al processo di rendicontazione nel rispetto dei codici di condotta e degli elementi di controllo relativi al processo di rendicontazione stabiliti nel presente documento.

In fase di chiusura della commessa/progetto, il Responsabile di commessa/progetto attesta l'effettivo completamento delle attività e la corretta produzione dei documenti di commessa/progetto in un rapporto finale di chiusura commessa/progetto. Tale rapporto viene sottoposto a validazione e firma da parte dell'Ufficio competente e, qualora previsto, del committente per l'attestazione di regolare esecuzione.

Devono essere **verbalizzate le attività di gestione della commessa** che prevedono **comunicazioni e/o incontri formali** con soggetti rappresentanti del committente, ad esempio in occasione della condivisione/approvazione di Stati Avanzamento Lavori o di prospetti rendicontativi.

Infratel Italia elabora dati accurati sulla presenza del personale aziendale impegnato nelle varie commesse, anche per mezzo di sistemi di rilevazione - timbratura badge, timesheet ed applicativi dedicati. Il personale è tenuto, utilizzando gli applicativi dedicati, attraverso le modalità e nel rispetto delle scadenze definite e comunicate dalla funzione Risorse Umane (svolta in service dalla Capogruppo), dunque **sulla base delle linee guida di Capogruppo** ed in coordinamento con le competenti funzioni della stessa, ad aggiornare costantemente la situazione presenze, inserendo in modo corretto e veritiero i giustificativi di presenza/assenza

[65] Unitamente al progetto esecutivo, all'atto di validazione e ad apposita relazione del Responsabile del Procedimento

occorrenti alla quadratura periodica.

I soggetti preposti all'approvazione delle presenze/assenze del personale autorizzano le presenze/assenze richieste dalle risorse e sono tenuti a verificare ed approvare i dati disponibili a sistema secondo le modalità e le scadenze definite e comunicate dalla funzione Risorse Umane presso la Capogruppo. Quest'ultima provvede, sulla base dei dati e dell'iter autorizzativo posto in essere, all'esatta contabilizzazione delle presenze/assenze del personale.

Il Referente di Contratto di Servizio/Amministratore Delegato garantisce il rispetto delle attività espletate dalla Capogruppo.

Infratel Italia elabora dati accurati relativi alle attività lavorative effettivamente svolte sulle commesse/progetto/piano, interne od esterne, in termini di ore lavorate dal personale aziendale anche attraverso l'impiego di idonei sistemi informatici dedicati. Gli Uffici a cui riferiscono i Responsabili di commessa/RUP competenti eseguono le opportune **verifiche dell'effettiva presenza del personale nei giorni di lavoro caricati a sistema e consuntivati sulla commessa**, anche attraverso la verifica periodica, almeno su base mensile, di coerenza tra le presenze/assenze del personale e le trasferte pianificate/consuntivate.

L'Amministratore Delegato, **avvalendosi della collaborazione della funzione Controllo di Gestione**, **stabilisce le opportune modalità operative per l'imputazione delle ore lavorate su ciascuna Commessa/Progetto** al fine di consentire l'esatta attribuzione dei costi rendicontabili al committente.

Il sistema informativo e di comunicazione di Infratel Italia **assicura** che l'**attribuzione** del tempo lavorato su ciascuna commessa sia **corretta e condivisa** dalle risorse direttamente coinvolte e **dai** Soggetti titolati alla verifica e approvazione, ossia i **Responsabili di Commessa/RUP**, **nonché** tempestiva per **il consolidamento dei dati contabili** e strumentali alla rendicontazione verso il committente. Il personale è tenuto alla corretta, veritiera e coerente imputazione del tempo effettivamente lavorato su ciascuna commessa aziendale, interna e/o esterna, utilizzando gli applicativi dedicati, attraverso le modalità operative stabilite e nel rispetto delle scadenze definite dall'Ufficio Controllo di Gestione.

I Responsabili preposti alla verifica del tempo lavorato sulla commessa sono tenuti a verificare, approvare o respingere quanto imputato dalle risorse, attraverso le modalità operative stabilite e nel rispetto delle scadenze definite. Eventuali errori accertati dovranno essere segnalati dal Responsabile e quindi corretti dalla risorsa interessata.

Infratel Italia assicura correttezza, trasparenza e tracciabilità nella gestione delle trasferte lavorative del proprio personale.

Le **trasferte** sono preliminarmente **pianificate dai Responsabili di Commessa/RUP** in relazione alle commesse di propria responsabilità. **Ciascuna trasferta**, per la quale deve sempre essere identificata la **commessa interna e/o esterna di riferimento**, viene richiesta dai soggetti interessati e sottoposta **all'approvazione del proprio Responsabile o del Responsabile di Commessa/Progetto se diverso**.

Le risorse interessate sono tenute alla corretta **rendicontazione delle spese sostenute** per la trasferta nel rispetto delle voci di spesa rimborsabili **definite in apposite policies interne, anche di gruppo**, attraverso la predisposizione di una nota spese, a cui devono essere allegati i relativi giustificativi fiscalmente validi, oggetto di verifica ed autorizzazione da parte dei Responsabili di Commessa/RUP.

La funzione Amministrazione e Bilancio presso la Capogruppo è tenuta ad effettuare il controllo dei rapporti e dei giustificativi verificando il rispetto delle policy aziendali e di gruppo.

In fase di chiusura dell'intervento, il Responsabile di commessa/RUP attesta l'effettivo completamento delle

attività e la corretta produzione dei documenti di commessa in un rapporto finale di chiusura commessa. Tale rapporto viene sottoposto a validazione e firma da parte del Responsabile dell'Ufficio e, qualora previsto, del committente per l'attestazione di regolare esecuzione.

Nel caso in cui siti di pertinenza di Infratel Italia siano sottoposti a sequestro, la funzione competente, ovvero il soggetto interno, formalmente identificato/incaricato dai Soggetti titolati della Società, a cui è affidata la custodia dei siti stessi, è tenuto, affinché ne sia preservata l'integrità, a prendere i dovuti provvedimenti atti a limitare l'accesso all'area sottoposta a sequestro al solo personale preventivamente autorizzato, anche tramite la segregazione della stessa per mezzo di opportuni dispositivi e l'apposizione di idonea segnaletica. Se ad essere sottoposti a sequestro sono beni mobili di proprietà aziendale, o comunque affidati in custodia alla Società, ovvero presenti in siti di sua pertinenza, la funzione competente, ovvero il referente interno, formalmente identificato/incaricato dai Soggetti titolati della Società, a cui è affidata la custodia degli stessi, è tenuto a prendere i dovuti provvedimenti al fine di impedirne l'uso, il danneggiamento o la sottrazione, anche tramite la segregazione dei beni confiscati per mezzo di opportuni dispositivi e l'apposizione di idonea segnaletica.

È fatto divieto a tutto il personale interessato alle attività in esame di appropriarsi indebitamente, anche temporaneamente, di materiali, beni e strumentazione della Società o di terzi.

Infratel Italia assicura che le attività di **manutenzione delle infrastrutture di rete** siano condotte in maniera corretta, trasparente e tracciabile, nel rispetto delle condizioni previste dagli accordi stipulati e della normativa vigente e applicabile alla Società.

Per ogni attività di manutenzione è individuato un Responsabile di commessa di manutenzione/RUP (di seguito anche "Manutenzione").

Il Responsabile di Manutenzione **assicura:**

- la **gestione tempestiva delle anomalie/malfunzionamenti di rete nel rispetto degli SLA contrattuali**, attraverso l'attivazione di ditte qualificate, nell'ambito di accordi contrattuali già in essere[66], quindi il successivo monitoraggio della corretta e tempestiva risoluzione delle anomalie in accordo ai requisiti contrattuali prestabiliti;
- **la tracciabilità delle richieste di intervento, l'attestazione di avvenuto intervento/ripristino** nonché la verifica delle attività di manutenzione correttiva effettivamente realizzate;

Al fine di verificare la corrispondenza di quanto consuntivato dalle ditte di manutenzione in tema di attività svolte e quanto effettivamente da queste realizzato, **Gestione Rete assicura**, anche per il tramite delle funzioni/referenti interni da questa identificati, in accordo al Responsabile di Manutenzione, la pianificazione e l'attuazione di **controlli a campione volti a verificare la correttezza dell'operato di dette ditte appaltatrici**. I **risultati di tali verifiche sono comunicati tempestivamente** a Gestione Rete ed all'Amministratore Delegato per le eventuali opportune azioni correttive.

Le **attività di manutenzione programmata** sono progettate/pianificate dal Responsabile di Manutenzione ed **autorizzate** da Gestione Rete e/o dalle funzioni/referenti interni da questa identificati. Le attività sono pianificate tenendo in considerazione anche quanto preventivato dalle ditte di manutenzione, previo sopralluogo preliminare qualora ritenuto opportuno in funzione della tipologia di intervento.

L'attivazione delle ditte appaltatrici avviene previo **riscontro di congruità economica** sulla base delle attività richieste dall'intervento e dei prezziari, o delle modalità di definizione del prezzo, definite nell'ambito di accordi contrattuali già in essere.

[66] Definiti nel rispetto degli elementi di controllo stabiliti per il processo di acquisto di servizi e lavori

Il Responsabile di Manutenzione certifica[67] **l'avvenuto intervento in accordo alle attività pianificate**, previo sopralluogo qualora ritenuto opportuno in funzione della tipologia dell'intervento, oggetto di approvazione da parte del Responsabile Unico del Progetto.

Gestione Rete e/o le funzioni/soggetti interni da questa identificati, in collaborazione con il Responsabile di Manutenzione, **individuano le tipologie di intervento manutentivo per le quali, in funzione della complessità e degli importi richiesti, è necessario prevedere sopralluoghi**:

- **preliminari** all'accettazione dei preventivi comunicati dalle ditte;
- preordinati alla **verifica di corretta prestazione** ed alla **successiva certificazione** di accettazione dell'intervento.

L'Ufficio Gestione Rete assicura inoltre, anche per il tramite delle funzioni/soggetti interni da questa identificati, la pianificazione e **l'attuazione di controlli a campione volti a verificare la correttezza dell'operato** delle ditte appaltatrici. I risultati di tali verifiche sono comunicati tempestivamente all'Amministratore Delegato o al soggetto titolato[68] per le eventuali opportune azioni correttive.

Il Responsabile di Manutenzione è tenuto ad inviare a Gestione Rete e/o alle funzioni/soggetti interni da questa identificati una reportistica periodica relativa al monitoraggio del servizio di manutenzione, indicativa degli SLA disattesi o che hanno raggiunto livelli di attenzione, delle azioni proposte o intraprese e dei possibili maggiori oneri economici derivanti dalle azioni richieste.

È fatto divieto a tutto il personale interessato alle attività in esame di appropriarsi indebitamente, anche temporaneamente, di materiali/strumentazioni della Società o di terzi.

Tutti gli attori coinvolti hanno l'obbligo di comunicare tempestivamente all'Organismo di Vigilanza deroghe, anomalie o atipicità eventualmente riscontrate rispetto alle determinazioni stabilite per il presente processo.

I responsabili di tutti gli Uffici sotto la responsabilità della divisione Infrastrutture e Operations sono tenuti, ciascuno per gli interventi di propria competenza, alla comunicazione periodica, su base semestrale, all'Organismo di Vigilanza, al RPCT e all'Amministratore delegato di un'informativa sullo stato di avanzamento d ciascuna commessa/progetto/piano.

Fermo restando l'obbligo in capo a tutti gli attori coinvolti, il RUP (scelto tra i diversi responsabili degli Uffici a seconda dell'ambito in cui rientra l'intervento, è, inoltre, tenuto alla comunicazione periodica, su base annuale, di un'informativa riepilogativa all'Organismo di Vigilanza, al RPCT e all'Amministratore delegato, delle varianti approvate nel periodo di riferimento con l'indicazione dell'importo, delle motivazioni e dei soggetti beneficiari con l'indicazione delle eventuali azioni correttive stabilite.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate, gli Uffici dell'Area Infrastrutture e Operations, insieme all'Ufficio Controllo di Gestione, sono tenuti alla comunicazione periodica, su base annuale all'OdV di un'informativa riepilogativa del tempo effettivamente lavorato su ciascuna commessa/progetto/piano aziendale da risorse interne.

Fermo restando l'obbligo, in capo a tutti gli attori coinvolti, di comunicare eventuali anomalie o atipicità riscontrate all'Organismo di Vigilanza ed al RPCT, l'Ufficio Gestione Rete è inoltre tenuto alla comunicazione periodica, su base annuale, di un'informativa riepilogativa dei dati relativi al servizio di manutenzione e dell'esito delle attività di verifica a campione sull'operato delle imprese affidatarie con l'indicazione delle eventuali azioni correttive stabilite.

[67] Anche attraverso il riscontro della documentazione ricevuta attestante le attività poste in essere
[68] Sulla base del sistema di procure e deleghe

In ogni caso, il responsabile di ciascun Ufficio dell'Area Infrastrutture e Operations, per le attività di rilievo di questa sezione del MOGC 231, comunica all'OdV e al RPCT, con cadenza almeno annuale, le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

V.5.10. ELEMENTI DI CONTROLLO PER GESTIONE SINFI

Relativamente al Progetto SINFI valgono gli elementi di controllo indicati per l'area **Ingegneria delle Reti e dei Sistemi** circa la gestione e la sicurezza dei sistemi informatici di proprietà aziendale. Inoltre, ai fini del corretto e legittimo accesso ai Sistemi informativi della Pubblica Amministrazione finalizzato alla gestione e al monitoraggio delle commesse/progetti, le funzioni competenti, in collaborazione con i Referenti interni per la gestione degli aspetti IT, ciascuno per gli aspetti di pertinenza, assicurano:

- un'adeguata gestione delle credenziali di accesso a detti sistemi;
- l'effettuazione di verifiche informatiche periodiche volte a garantire che l'accesso effettivo ai sistemi informatici della PA sia effettuato in funzione delle procure in essere, al fine di assicurare la completezza, l'accuratezza e la veridicità della documentazione/dati/informazioni da trasmettere o ricevere (trasmissione telematica dei dati, in modo particolare se corredata di autenticazione o firma digitale, invio dei file prodotti da elaborazioni on line, etc.).

L'Ufficio SINFI è tenuto alla comunicazione periodica, su base annuale, di un'informativa riepilogativa all'OdV e al RPCT di eventuali anomalie rilevate durante la gestione del sistema Sinfi.
In ogni caso, il responsabile dell'Ufficio SINFI comunica all'OdV e al RPCT, con cadenza almeno annuale, le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).

V.5.11. ELEMENTI DI CONTROLLO PER GESTIONE PIANO ISOLE MINORI.

Il Piano Isole Minori prevede la realizzazione di infrastrutture terrestri e sottomarine per la realizzazione del collegamento in fibra ottica delle isole.
In ragione della peculiarità della lavorazione e della responsabilità diretta di Infratel Italia rispetto all'operato dell'affidatario del servizio/appalto, sono previste specifiche misure a tutela dei lavoratori e per la verifica di qualità del servizio.
Per le verifiche in campo, ciascun responsabile di funzione e/o di commessa/progetto autorizza la trasferta del personale ad esso assegnato avendo preventivamente verificato che, per lo stesso, sia stata effettuata la formazione/addestramento, sia stata valutata l'idoneità a valle delle visite mediche preventive e siano stati forniti, o si rendano disponibili, tutti i DPI necessari per operare nel luogo di destinazione comprendendo la tessera di riconoscimento.
Per le attività marine il personale dovrà, in aggiunta:

- aver preso visione dell'informativa sulla normativa vigente in materia di lavori marittimi, predisposta dal RSPP di Infratel Italia;
- ricevere, da parte del Comandante della nave che lo ospiterà o da suo delegato, l'informazione sulle procedure d'emergenza e i rischi specifici presenti a bordo della nave e ricevere, i DPI eventualmente indicati nelle stesse.

A verifica dei punti precedentemente indicati, il RUP invierà una mail all'ufficio Qualità Privacy e Sicurezza relativa al proprio personale indicando l'avvenuta informazione/presa visione della documentazione SSL fornita.
In capo agli affidatari è altresì previsto, mediante apposite clausole contrattuali, il rispetto di specifiche misure per il rispetto dei beni culturali e ambientali. Nessun lavoro può essere eseguito in assenza delle prescritte

autorizzazioni. In caso di ritrovamento di reperti sono avvisate le competenti autorità per le necessarie operazioni.

Tutti i destinatari del Modello ex d.lgs. n. 231/2001 e del Piano Prevenzione della Corruzione e della Trasparenza (PPCT), adottato ai sensi della Legge n. 190/2012, sono obbligati a comunicare in modo tempestivo all'OdV e alla funzione RPCT anomalie o atipicità eventualmente riscontrate rispetto alla procedura e tutti i fatti, atti o omissioni che possano incidere sull'osservanza dei citati documenti.
L'area Operations Isole è tenuta, almeno su base annuale, a inviare un'informativa riepilogativa all'OdV e al RPCT delle verifiche effettuate e di eventuali anomalie rilevate durante la gestione del Piano.

In ogni caso, il responsabile dell'Ufficio Operations Isole comunica all'OdV e al RPCT, con cadenza almeno annuale, le non conformità riscontrate, attestando, in caso negativo, l'assenza di eventi critici (positive assurance).