AVVISO

CONSULTAZIONE PRELIMINARE DI MERCATO

Oggetto

Consultazione preliminare di mercato per l'eventuale affidamento della fornitura di una piattaforma per la Due Diligence propedeutica all'affidamento di un appalto avente ad oggetto prestazioni non strumentali allo svolgimento dell'attività di trasporto ferroviario.

I. Premessa

In applicazione dei principi di buona amministrazione, non discriminazione e trasparenza**, Ferservizi S.p.A.**, con sede in Piazza della Croce Rossa 1, 00161 Roma – capitale sociale Euro 8.170.000,00 partita IVA, Codice Fiscale e numero di iscrizione al Registro delle Imprese 04207001001, in nome e per conto di FSTechnology S.p.A. (di seguito anche "Ferservizi"), ha l'obiettivo di:

- garantire la massima pubblicità alle iniziative per assicurare la più ampia diffusione delle informazioni ed un celere svolgimento delle eventuali successive procedure di acquisto;
- ottenere la più proficua partecipazione da parte degli Operatori economici interessati a partecipare alla presente consultazione preliminare di mercato (di seguito anche "Consultazione");
- pubblicizzare al meglio le caratteristiche qualitative e tecniche del prodotto oggetto di Consultazione;
- ricevere, da parte dei soggetti interessati, osservazioni e suggerimenti per una più compiuta conoscenza del mercato;
- individuare le migliori soluzioni di mercato, con alto contenuto innovativo e forte impatto in termini di efficacia ed efficienza della soluzione proposta, di vantaggio o riduzione di impatti ambientali o sociali rivolti ai propri dipendenti, ai clienti o alla collettività;

Oggetto della presente Consultazione è l'affidamento della fornitura della piattaforma per la Due Diligence (di seguito "Appalto"), rispetto al quale - previa presa visione dell'informativa sul trattamento dei dati personali pubblicata secondo le modalità di cui al successivo Paragrafo IX - Vi chiediamo di fornire il Vostro contributo compilando il questionario allegato al presente Avviso di cui agli Allegati 1 e 1.1; il questionario dovrà essere inviato secondo i termini e le modalità indicate al successivo Paragrafo VI.

Il Gestore del presente procedimento è Giovanni Gervasoni.

La presente procedura ha ad oggetto prestazioni non strumentali allo svolgimento dell'attività di trasporto ferroviario e pertanto il suo successivo eventuale affidamento non sono sottoposti alla disciplina pubblicistica in materia di contratti pubblici.

Per la disciplina dell'eventuale affidamento, pertanto, trovano applicazione le disposizioni del Codice Civile; nonché leggi speciali o altre disposizioni di legge vigenti in materia di contratti di diritto privato.

II. Scopo della Consultazione

La presente consultazione preliminare di mercato ha la specifica finalità di raccogliere informazioni utili per la preparazione dell'Appalto ai fini del perfezionamento delle specifiche tecniche propedeutiche all'eventuale indizione di una successiva procedura di selezione da espletarsi in conformità alle disposizioni di legge vigenti in materia di contratti di diritto privato.

Pertanto, la presente Consultazione, è volta a:

- rendere noti i requisiti minimi tecnico – funzionali richiesti per l'eventuale successivo futuro affidamento dell'Appalto di cui si ritiene necessario il possesso da parte degli Operatori economici esperti dello specifico settore di mercato;
- agevolare la preparazione dell'Appalto, mediante la ricezione, da parte degli Operatori economici che manifestino interesse a partecipare alla presente Consultazione, di contributi utili per il perfezionamento delle specifiche tecniche propedeutiche all'eventuale successiva indizione di una procedura di selezione da espletarsi in base alla disciplina di cui sopra;
- avviare un dialogo informale con gli Operatori economici partecipanti alla Consultazione, onde ricevere dai medesimi osservazioni, suggerimenti e informazioni circa ulteriori specifiche tecniche dell'Appalto.

III. Descrizione dell'oggetto dell'iniziativa e Requisiti minimi tecnico – funzionali

La società FSTechnology del Gruppo FS ha avviato un progetto per l'acquisto di una piattaforma software che supporti la Struttura Compliance di Ferrovie dello Stato Italiane spa per la gestione dei processi di Due Diligence su Terze Parti.

Si rimanda all'Allegato 2 al presente Avviso per la descrizione di dettaglio del prodotto della presente Consultazione e dei relativi requisiti tecnico-funzionali minimi richiesti che l'oggetto dell'Appalto dovrà soddisfare.

In particolare, sarà cura dell'Operatore economico compilare i questionari riportati nei succitati Allegati 1 e 1.1.

IV. Durata e importo stimato della successiva eventuale procedura di selezione

L'appalto al quale è propedeutica la presente Consultazione avrà una durata prevista di 60 mesi, nel corso dei quali è prevista una spesa di importo massimo complessivo pari ad € 800.000,00 IVA esclusa.

V. Requisiti di Partecipazione

Si precisa che ai fini della successiva eventuale procedura di selezione che potrà essere indetta per l'affidamento della piattaforma oggetto della presente Consultazione, nonché per la stipula del relativo eventuale Accordo Quadro, il/gli Operatore/i economico/i non dovrà/anno trovarsi nelle seguenti cause ostative alla stipula del rapporto contrattuale. In particolare, si rappresenta che costituiscono cause ostative alla stipula dell'Accordo Quadro:

1. L'aver subito condanna con sentenza definitiva o decreto penale di condanna divenuto irrevocabile o sentenza di applicazione della pena su richiesta ai sensi dell'articolo 444 del codice di procedura penale, per uno dei seguenti reati:

   a) delitti, consumati o tentati, di cui agli articoli 416, 416-bis del codice penale ovvero delitti commessi avvalendosi delle condizioni previste dal predetto articolo 416-bis ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo, nonché per i delitti, consumati o tentati, previsti dall'articolo 74 del D.P.R. n. 309/1990, dall'articolo 291-quater del D.P.R. n. 43 del 1973 e dall'articolo 260 del D.Lgs. n. 152/2006, in quanto riconducibili alla partecipazione a un'organizzazione criminale, quale definita all'articolo 2 della decisione quadro 2008/841/GAI del Consiglio dell'Unione Europea;

   b) delitti, consumati o tentati, di cui agli articoli 317, 318, 319, 319-ter, 319-quater, 320, 321, 322, 322-bis, 346-bis, 353, 353-bis, 354, 355 e 356 del codice penale nonché all'articolo 2635 del codice civile;

   b-bis) false comunicazioni sociali di cui agli articoli 2621 e 2622 del codice civile;

   c) frode ai sensi dell'articolo 1 della convenzione relativa alla tutela degli interessi finanziari delle Comunità europee;

   d) delitti, consumati o tentati, commessi con finalità di terrorismo, anche internazionale, e di eversione dell'ordine costituzionale, reati terroristici o reati connessi alle attività terroristiche;

   e) delitti di cui agli articoli 648-bis, 648-ter e 648-ter.1 del codice penale, riciclaggio di proventi di attività criminose o finanziamento del terrorismo, quali definiti all'articolo 1 del decreto legislativo 22 giugno 2007, n. 109 e successive modificazioni;

   f) sfruttamento del lavoro minorile e altre forme di tratta di esseri umani definite con il decreto legislativo 4 marzo 2014, n. 24;

   g) ogni altro delitto da cui derivi, quale pena accessoria, l'incapacità di contrattare con la pubblica amministrazione.

I reati di cui al precedente punto 1. costituiscono causa ostativa quando riguardano anche uno soltanto dei seguenti soggetti, esclusi i cessati dalla carica:

- in caso di impresa individuale, il titolare, il direttore tecnico (se presente);
- in caso di società in nome collettivo, i soci, il direttore tecnico (se presente);
- in caso di società in accomandita semplice, i soci accomandatari, il direttore tecnico (se presente);
- se si tratta di altro tipo di società o di un consorzio, gli amministratori o in alternativa i membri del consiglio di gestione muniti di potere di rappresentanza; il direttore tecnico (se presente); il socio unico persona fisica, ovvero il socio di maggioranza persona fisica in caso di società con un numero di soci pari o inferiore a quattro; il procuratore dell'Operatore economico che sottoscrive l'eventuale l'offerta e/o il contratto a valle dell'eventuale successiva procedura di affidamento.

2. la sussistenza di una delle cause di decadenza, di sospensione o di divieto previste dall'art. 67 del D.Lgs. n. 159/2011 e s.m.i. o un tentativo di inflazione mafiosa di cui all'art 84, comma 4 del medesimo decreto quando riguardano anche uno solo dei soggetti sopra richiamati;
3. la sussistenza di gravi violazioni agli obblighi relativi al pagamento delle imposte e tasse o dei contributi previdenziali;

4. la commissione di gravi infrazioni alle norme in materia di sicurezza e ad ogni altro obbligo derivante dai rapporti di lavoro, nonché agli obblighi di legge in materia ambientale, sociale e del lavoro;
5. nel caso in cui l'Operatore economico sia stato sottoposto a fallimento o si trovi in stato di liquidazione coatta o di concordato preventivo o sia in corso nei suoi confronti un procedimento per la dichiarazione di una di tali situazioni, fermo restando quanto previsto dall'art 110 del d.lgs. 18 aprile 2016, n. 50, convenzionalmente applicabile, e dall'articolo 186-bis del regio decreto 16 marzo 1942, n. 267;
6. la carenza di affidabilità professionale, nei casi in cui l'Operatore economico si sia reso colpevole – secondo motivata valutazione della scrivente e/o di FS in ordine alla permanenza o meno del necessario rapporto fiduciario tra committente e appaltatore – di gravi illeciti professionali tali da renderne dubbia l'integrità o l'affidabilità, per essere incorsi, negli ultimi tre anni, a titolo esemplificativo:

   i. nella risoluzione per inadempimento di contratti di appalto di lavori, servizi e forniture affidati dalla scrivente e/o da FS e/o da altre Società del Gruppo Ferrovie dello Stato Italiane;

   ii. nella dichiarata non collaudabilità di lavori, servizi e forniture oggetto di un contratto stipulato con la scrivente e/o con FS e/o con altra Società del Gruppo Ferrovie dello Stato Italiane SpA;

   iii. nella violazione, nel corso dell'esecuzione di precedenti contratti ovvero in occasione della partecipazione a precedenti procedure di gara, di qualsiasi delle norme contenute nel Codice Etico del Gruppo Ferrovie dello Stato Italiane, accertata con qualsiasi mezzo di prova dalla scrivente e/o da FS e/o da altra Società del Gruppo Ferrovie dello Stato Italiane SpA;

   iv. nella mancata stipula del Contratto o presa in consegna di lavori, forniture o servizi affidati dalla scrivente e/o da FS e/o da altra Società del Gruppo Ferrovie dello Stato Italiane, per fatto e colpa dell'Operatore Economico in epigrafe.

Le cause ostative alla stipula del Contratto previste ai precedenti Punti non si applicano alle aziende o società sottoposte a sequestro o confisca ai sensi dell'articolo 12-sexies del D.L. n. 306/1992, convertito, con modificazioni, dalla legge n. 356/1992 o degli articoli 20 e 24 del D. Lgs. n. 159/2011, ed affidate ad un custode o amministratore giudiziario o finanziario, limitatamente a quelle riferite al periodo precedente al predetto affidamento.

I reati di cui al precedente Punto 1 non costituiscono causa ostativa alla stipula del Contratto laddove depenalizzati, ovvero estinti dopo la condanna, ovvero in caso di revoca della condanna medesima, ovvero laddove sia intervenuta la riabilitazione, ovvero nei casi di condanna ad una pena accessoria perpetua, quando questa è stata dichiarata estinta ai sensi dell'articolo 179, settimo comma, del codice penale.

La verifica dell'assenza delle cause ostative di cui ai precedenti punti 1. e 2., avverrà a valle dell'eventuale successiva procedura di selezione, mediante espletamento di un'indagine reputazionale nei confronti del relativo Operatore economico.

VI. Modalità di partecipazione alla Consultazione e tipologia di contributi ammessi

L'iniziativa è rivolta a tutti coloro che siano in possesso di informazioni rilevanti per le finalità descritte nel presente Avviso e, pertanto, tutti i soggetti interessati a partecipare alla presente Consultazione

potranno fornire contributi di carattere tecnico mediante la compilazione del questionario di cui ai succitati Allegati 1e 1.1.

Per partecipare alla Consultazione gli Operatori economici dovranno compilare il Modulo denominato "Manifestazione di Interesse alla Consultazione" di cui all'Allegato 1, il "Questionario" di cui all'Allegato 1.1 e trasmetterli nelle modalità descritte al presente Paragrafo.
Ciascun Operatore economico interessato dovrà - **preventivamente ed obbligatoriamente** - richiedere la registrazione al Portale Acquisti di Ferservizi (di seguito, per brevità, "Portale"), ove non già in possesso di apposita utenza di accesso al Portale.
Per ottenere la registrazione al Portale, gli Operatori economici dovranno collegarsi al sito www.acquistionlineferservizi.it, accedere al Portale, scaricare il file denominato "MODULO DI ADESIONE AL PORTALE ACQUISTI", completare la registrazione cliccando su nuova registrazione fornitore e allegare il suddetto file firmato digitalmente dal Legale Rappresentante dell'Operatore economico, unitamente alla scansione di un documento di identità, in corso di validità, del Legale Rappresentante.
Nella sezione istruzioni del Portale è presente una guida dettagliata delle operazioni sopra descritte.
Si precisa che i tempi tecnici legati alle attività di registrazione sono stimati in **circa 24 ore.**
La registrazione al Portale è a titolo gratuito.
I dati di registrazione sul Portale agevolano la corrispondenza con Ferservizi; i riferimenti dell'Operatore economico dovranno contenere obbligatoriamente un indirizzo e-mail di posta certificata che varrà quale strumento di comunicazione con Ferservizi.
In caso di necessità di supporto ai fini della registrazione al Portale, nonché nello svolgimento delle operazioni all'interno del Portale stesso, gli Operatori economici concorrenti hanno facoltà di contattare il Servizio Assistenza al numero dedicato **+39 02 00 70 42 52**.
Al fine di poter rispondere al presente avviso, gli Operatori economici dovranno essere in possesso della seguente dotazione tecnica minima:

- **Indirizzo di Posta Elettronica Certificata (PEC);**
- **Certificato di firma digitale**, per ciascuno dei soggetti firmatari in corso di validità, rilasciato da un organismo incluso nell'elenco pubblico dei certificatori tenuto da AgID (previsto dall'art. 29, comma 1 del D.Lgs. 82/2005) generato mediante un dispositivo per la creazione di una firma sicura, ai sensi di quanto previsto dall'art. 38, comma 2 del D.P.R. 445/2000 e dall'art. 65 del D.Lgs. 82/2005.
- Personal Computer collegato ad Internet con le seguenti caratteristiche: AMBIENTI MS Windows XP, Windows 7 o Vista; COLLEGAMENTO A INTERNET connessione ADSL con una banda minima effettiva di 1MB (ADSL) o superiore o connessione internet aziendale (si raccomanda di consultare il personale IT interno per verificare l'effettiva disponibilità di banda e la possibilità di accesso in base alle configurazioni di proxy/firewall); WEB BROWSER Internet Explorer 7 (Consigliato) o superiore, Mozilla, Firefox o Google Crome; JAVA VIRTUAL MACHINE Plug-in SUN 1.6 o superiore.

All'interno della sezione Requisiti minimi hw e sw del Portale è possibile verificare la corretta configurazione del proprio personal computer.

****

MODALITÀ DI PRESENTAZIONE DELLA MANIFESTAZIONE DI INTERESSE

Al completamento delle operazioni di registrazione gli Operatori economici interessati per rispondere alla presente Consultazione dovranno:

- accedere al Portale (previa attivazione di apposita user ID, inserita in fase di registrazione, e password, ricevuta tramite comunicazione e-mail di sistema e modificabile in fase di accesso), nella sezione fasi di prequalifica (FDP) e poi cliccare su eventi ad evidenza pubblica;
- accedere all'Avviso telematico *de quo*;
- selezionare il tasto partecipa;
- (solo al primo accesso) cliccare su mia risposta, posto sulla sinistra della pagina web;
- (solo al primo accesso) cliccare sul link "Rispondi" (posizionato al centro dello schermo) per avviare il processo di risposta.

Ultimate tali operazioni gli Operatori economici potranno scaricare l'ulteriore documentazione relativa al presente avviso, porre chiarimenti, ricevere le risposte e presentare quanto necessario in risposta alla presente Consultazione.

Per redigere le relative dichiarazioni nonché per caricare l'eventuale documentazione a corredo l'Operatore economico dovrà, all'interno della Busta amministrativa digitale, allegare i documenti richiesti, sottoscritti con firma digitale.

Si precisa che tutti i file allegati al Portale (dichiarazioni e/o documenti scansionati) dovranno essere firmati digitalmente e non potranno essere superiori ai 10 Mb, pena il mancato controllo della firma digitale.

Si ricorda che non è consentito firmare digitalmente una cartella compressa (es. zip) contenente documenti privi di firma digitale, ma è possibile allegare una cartella compressa contenente documenti digitalmente firmati.

Al termine dell'inserimento della documentazione richiesta, l'Operatore economico dovrà cliccare su "Salva ed Esci" per salvare quanto inserito e tornare alla propria pagina riepilogativa della fase di prequalifica.

Una volta espletate tali attività l'Operatore economico concorrente dovrà cliccare su *Trasmetti risposta*.

L'Operatore economico potrà visualizzare nella sua cartella personale, alla colonna Stato della risposta, l'avvenuta trasmissione (Stato della risposta: *trasmessa*).

L'Operatore economico potrà modificare i dati precedentemente trasmessi ovvero ritirare la propria risposta entro e non oltre la data e l'ora di scadenza di cui in seguito.

DOCUMENTI DA ALLEGARE

Gli Operatori economici interessati a partecipare alla presente Consultazione possono manifestare il proprio interesse inviando, sul Portale, entro e non oltre il giorno 26/06/2023 ore 13:00 quanto segue:

a) Modulo denominato "Manifestazione di Interesse alla Consultazione", da rendere compilando il *facsimile* Allegato 1, firmato dal legale rappresentante dell'Operatore economico che la rende;
b) Modulo denominato "Questionario", da rendere compilando il *facsimile* Allegato 1.1;
c) Caricare un Proof of Concept (PoC) per ognuno degli use case descritti nell'Allegato 1.2;
d) E' possibile caricare eventuali altri documenti facoltativi.

N.B. Tutta la documentazione deve essere redatta in **lingua italiana**. In caso contrario, tutta la documentazione deve essere accompagnata da traduzione in lingua italiana certificata "conforme al testo straniero" dalla competente rappresentanza diplomatica o consolare ovvero da un traduttore ufficiale.

Tutti i file allegati al Portale (dichiarazioni e/o documenti scansionati) dovranno essere firmati digitalmente dal rappresentante legale dell'Operatore economico partecipante o procuratore munito di appositi poteri.

N.B. Alla manifestazione di interesse alla Consultazione NON dovrà essere allegata alcuna offerta economica.

L'invio telematico della manifestazione di interesse alla Consultazione è a totale ed esclusivo rischio del mittente, restando esclusa qualsivoglia responsabilità di Ferservizi, ove, per qualsiasi malfunzionamento alla struttura tecnica, tecnologia o di connessione dell'Operatore economico, la stessa non pervenga entro il termine di scadenza e secondo le modalità previste. Si invitano pertanto gli Operatori economici interessati ad avviare le attività finalizzate alla trasmissione di quanto richiesto con largo anticipo rispetto alla scadenza prevista onde evitare la non completa e quindi mancata trasmissione della risposta decorso tale termine.

N.B.: Qualora sia accertata la mancanza, l'incompletezza o l'irregolarità essenziale della documentazione presentata, si procederà alla richiesta di integrazione o di regolarizzazione di detta documentazione.

VII. Modalità di svolgimento della Consultazione preliminare di mercato

La Consultazione potrà svolgersi in fasi successive. Gli Operatori economici sono invitati a prendere visione della documentazione allegata al presente avviso.
Le manifestazioni di interesse ricevute saranno raccolte e analizzate da Ferservizi, ivi inclusa tutta la documentazione prodotta dagli Operatori Economici in riscontro alla presente Consultazione.
In base alle risultanze delle attività di analisi condotte ed al fine di acquisire tutte le informazioni e documentazioni utili per la migliore preparazione dell'Appalto ai fini della successiva eventuale indizione della relativa procedura di selezione, Ferservizi potrà eventualmente procedere ad invitare gli Operatori economici che hanno presentato manifestazione di interesse ad uno o più incontri di approfondimento tecnico. Tali incontri saranno oggetto di apposita verbalizzazione.
Per ogni fase di svolgimento della Consultazione, gli Operatori economici partecipanti riceveranno apposita comunicazione (a mezzo di pubblicazione di avvisi sul Portale e/o sul profilo committente).
Al termine della Consultazione, Ferservizi pubblicherà sul Portale e sul Profilo committente apposito avviso di chiusura della consultazione preliminare di mercato.

VIII. Riserve e precisazioni

La partecipazione alla presente Consultazione preliminare di mercato non dà diritto ad alcun compenso e/o rimborso per le spese sostenute, deve pertanto intendersi a titolo completamente gratuito.

Il presente Avviso, in quanto costituente avvio di una mera consultazione preliminare di mercato, non è vincolante e non è finalizzato all'assegnazione e stipula di alcun contratto, pertanto, la presente Consultazione non comporta alcun obbligo per Ferservizi di avviare procedure di selezione del contraente per le prestazioni oggetto dell'iniziativa.

La partecipazione alla consultazione preliminare di mercato:

- è ininfluente (ossia: non assicura e non preclude) rispetto alla partecipazione alla eventuale successiva procedura di selezione per l'affidamento dell'Appalto, non costituendo condizione di accesso, né titolo preferenziale, né impegno alcuno circa il prosieguo della procedura;
- non potrà, in alcun modo, ostacolare altri Operatori economici che non abbiano partecipato alla Consultazione avviata con il presente avviso;

- non determina alcuna aspettativa nei confronti di Ferservizi e gli Operatori economici non possono rivendicare alcun diritto al riguardo.

Tutte le informazioni da Voi fornite in riscontro al presente documento saranno utilizzate ai soli fini dello sviluppo dell'iniziativa in oggetto e non dovranno costituire offerte tecniche o economiche; a tal fine i contributi trasmessi non dovranno fornire anticipazioni in merito alle quotazioni afferenti il prodotto oggetto della presente Consultazione, al fine di non alterare il regolare sviluppo competitivo della successiva eventuale fase di selezione.
Pertanto, tutta la documentazione raccolta potrà essere utilizzata per la predisposizione della documentazione dell'eventuale successiva procedura di selezione per l'affidamento dell'Appalto, nei limiti del rispetto dei diritti di privativa e della proprietà intellettuale, di non discriminazione e di trasparenza.
Per tale motivo, al fine di garantire il rispetto del principio dell'effettiva concorrenza, Ferservizi potrà comunicare agli altri candidati e offerenti nell'ambito dell'eventuale successiva procedura di selezione, le informazioni pertinenti, scambiate nel quadro della presente Consultazione.
Ciò premesso, si invita a non inviare informazioni che contengano informazioni e/o dati protetti da diritti di privativa o da diritti di proprietà intellettuale comunque rilevatori di segreti aziendali, commerciali, tecnici o industriali, ovvero di inviare motivata e comprovata dichiarazione per la parte delle informazioni e/o documentazioni inviate per le quali si richiede la non divulgazione.
Si precisa, in vista dell'eventuale accesso da parte di altri Operatori economici agli esiti della presente Consultazione, che la divulgazione di quanto contenuto nei Vostri contributi avverrà in forma anonima.
Resta ferma la facoltà di Ferservizi di interrompere, modificare, prorogare, sospendere e revocare la procedura in qualsiasi momento, senza che ciò possa costituire, in alcun modo, diritto o pretesa a qualsivoglia risarcimento o indennizzo.

La consultazione preliminare di mercato si espleta nella piena osservanza del Codice Etico del Gruppo Ferrovie dello Stato Italiane, pubblicato al seguente indirizzo Internet: http://www.fsitaliane.it nella sezione "Il Gruppo FS" sottosezione "Governance", sottosezione "Codice etico" e nell'osservanza del Modello di Organizzazione, Gestione e Controllo ex D.lgs. n. 231/2001 e s.m.i. di FSTechnplogy ("Modello 231"), disponibile al seguente indirizzo Internet: http://www.fstechnology.it nella sezione "Chi siamo" sottosezione "Etica, compliance e integrità".

IX. Trattamento dei dati personali

Le Parti (Ferservizi, FSTechnology e ciascun Operatore economico) si impegnano a trattare i dati personali, acquisiti nell'ambito e per le finalità connesse alla presente Consultazione, nel rispetto dei principi di correttezza, liceità e trasparenza previsti dalla normativa vigente in materia di protezione dei dati personali (Regolamento UE 2016/679 e dal D.Lgs. n. 196/2003 e s.m.i.).
In particolare, le Parti si impegnano a trattare i dati personali nel rispetto del principio di minimizzazione, nonché a garantirne l'integrità e la riservatezza.
È fermo l'obbligo di ciascuna delle Parti, in qualità di Titolari autonomi del trattamento, di fornire l'informativa sul trattamento dei dati personali alle persone fisiche della propria organizzazione e a quelle dell'altra Parte i cui dati siano trattati per le finalità di cui al primo capoverso del presente Paragrafo e garantire l'esercizio dei diritti degli interessati.
L'obbligo di informativa di cui al terzo comma viene assolto da Ferservizi mediante pubblicazione nella sezione "Protezione dati personali" del sito istituzionale www.ferservizi.it. L'obbligo di

informativa è inoltre assolto dalle Società del Gruppo FS Italiane Titolari del trattamento mediante pubblicazione sui rispettivi siti istituzionali.
Ciascuna Parte risponde delle contestazioni, azioni o pretese avanzate da parte degli interessati e/o di qualsiasi altro soggetto e/o Autorità in merito alla inosservanza alla normativa vigente in materia di protezione dei dati personali (Regolamento UE 2016/679 e dal D.Lgs. 196/2003 e s.m.i.), ad essa ascrivibili.

X. Pubblicità

Il presente avviso e i relativi allegati sono pubblicati sul Portale Acquisti di Ferservizi raggiungibile al sito www.acquistionlineferservizi.it, nonché sul profilo del committente all'indirizzo www.ferservizi.it, nella sezione "Bandi e gare" – "Bandi FSTechnology" – "Servizi".
Al termine della Consultazione, Ferservizi pubblicherà sul Portale apposito avviso di chiusura della consultazione preliminare di mercato.

Si allegano:

Allegato 1: Manifestazione di Interesse alla Consultazione;
Allegato 1.1: Questionario;
Allegato 1.2: Progetto Digital Due Diligence - Use Case;
Allegato 2: Specifiche Tecniche.

Area Acquisti di Gruppo

Il Responsabile

Firmato digitalmente da

GENNARO RANIERI

CN = GENNARO RANIERI
O = FERSERVIZI S.p.A.
C = IT

Allegato 1

Manifestazione di Interesse alla consultazione

(Dichiarazione resa ai sensi e per gli effetti di cui agli artt. 46 e 47 del D.P.R. 445/2000 e s.m.i., ovvero, per gli Operatori economici stabiliti in stati diversi dall'Italia, documentazione equivalente secondo la legislazione dello stato di appartenenza e, comunque, nel rispetto di quanto previsto nell'art. 3, commi 2, 3 e 4 del D.P.R. n.445/2000 e s.m.i., e laddove applicabile, nel rispetto di quanto previsto nell'art, 33 del medesimo decreto.)

NOTE DI COMPILAZIONE: si invita a compilare le caselle in grigio. Il documento dovrà essere sottoscritto digitalmente, pertanto non è necessario apporre timbro e firma autografa.

Oggetto: Avviso Consultazione preliminare di mercato indetta per l'eventuale affidamento della fornitura di una piattaforma per la Due Diligence.

Il/la sottoscritto/a					
Nato/a a		**Prov.**	**( )**	**il**	**/ / /**
C.F.					
In qualità di:					
ovvero					
☐	**Procuratore (*in tal caso indicare gli estremi della relativa procura*)**				
della Società (indicare Ragione Sociale per esteso):					
C.F		**P.IVA**			
con sede legale in:					
Via				**n°**	
C.A.P.		**Città**		**Prov.**	**( )**
Telefono		**Fax**		**e-mail**	

MANIFESTA

il proprio interesse relativamente alla consultazione preliminare di mercato in oggetto per le finalità indicate al Paragrafo II dell'Avviso di Consultazione preliminare di mercato.

A tal fine, **consapevole, *ai sensi e per gli effetti dell'art.76 del d.P.R. 28 dicembre 2000, n. 445 e s.m.i., delle responsabilità e delle sanzioni previste in caso di dichiarazioni mendaci e/o formazione o uso di atti falsi, nonché in caso di esibizione di atti contenenti dati non più corrispondenti a verità e consapevole che qualora emerga la non veridicità del contenuto della presente dichiarazione decadrà dai benefici per i quali la stessa è rilasciata***

AI SENSI DEGLI ARTT. 46 E 47 DEL D.P.R. 445/2000

DICHIARA SOTTO LA PROPRIA RESPONSABILITA'

Sezione I

- di aver preso piena conoscenza e di accettare integralmente il contenuto dell'Avviso di consultazione di mercato e degli eventuali chiarimenti resi;
- che l'Impresa è iscritta nel registro della Camera di Commercio, Industria, Artigianato e Agricoltura (o ad altro organismo equipollente secondo la legislazione dello Stato di appartenenza) per attività inerente all'oggetto delle prestazioni da affidare e che:
- di essere consapevole che, in sede di partecipazione all'eventuale procedura di selezione, all'atto di presentazione dell'offerta, l'Impresa dovrà attestare l'assenza delle cause ostative indicate nell'Avviso in riferimento;

Sezione II – Requisiti minimi tecnico - funzionali

Si richiede di comunicare le informazioni generali ed il livello di copertura dei requisiti vincolanti con la indicazione di eventuali note compilando le seguenti schede dell'Allegato 1.1 Schema di risposta:

- Riferimenti Operatore Economico;
- Requisiti vincolanti.

Sezione III – Questionario tecnico

Si richiede di comunicare la valutazione di copertura dei requisiti migliorativi con la indicazione di eventuali note compilando la seguente scheda dell'Allegato 1.1 Schema di risposta:

- Requisiti migliorativi

Si richiede agli Operatori Economici di predisporre una dimostrazione delle funzionalità ed eventualmente uno o più documenti che permettano di verificare gli ambiti funzionali elencati nel foglio "POV" dell'Allegato 1.1 e descritti nell'Allegato 1.2

A tal fine gli Operatori Economici dovranno presentare gli elaborati (video o audiovideo) entro il termine di scadenza della RFI fissato per il 26/06/2023, è consentita la possibilità di integrare gli elaborati inviati con dei documenti.

Si ricorda che l'estrazione delle informazioni deve essere imputata al 19/06/2023, settimo giorno solare antecedente alla data corrispondente alla chiusura della presente RFI.

Sezione IV

Inoltre, **DICHIARA:**

A. di accettare che la presente Consultazione preliminare di mercato non dà diritto ad alcun compenso e/o rimborso per le spese sostenute, e che pertanto, ogni contributo viene reso a titolo completamente gratuito;
B. di accettare integralmente, senza condizione o riserva alcuna, che l'Avviso in riferimento, in quanto costituente avvio di una mera consultazione preliminare di mercato, non è vincolante e non è finalizzato all'assegnazione e stipula di alcun contratto, pertanto, la Consultazione non comporta alcun obbligo per Ferservizi di avviare procedure di selezione del contraente per le prestazioni oggetto dell'iniziativa. L'operatore economico, pertanto prende atto e accetta che:
    1. la partecipazione alla consultazione preliminare di mercato è ininfluente (ossia: non assicura e non preclude) rispetto alla partecipazione alla eventuale successiva procedura di selezione per l'eventuale affidamento dell'Appalto, non costituendo condizione di accesso, né titolo preferenziale, né impegno alcuno circa il prosieguo della procedura;
    2. non potrà, in alcun modo, ostacolare altri Operatori economici che non abbiano partecipato alla Consultazione avviata con il presente avviso;
    3. non determina alcuna aspettativa nei confronti di Ferservizi e gli Operatori economici non possono rivendicare alcun diritto al riguardo.
C. di accettare integralmente, senza condizione o riserva alcuna, che i contributi dallo stesso forniti potranno essere utilizzati per la predisposizione della documentazione dell'eventuale successiva procedura di selezione per l'affidamento dell'Appalto, nei limiti del rispetto dei diritti di privativa e della proprietà intellettuale[1], di non discriminazione e di trasparenza;
D. di accettare integralmente, senza condizione o riserva alcuna, che Ferservizi ha la più ampia facoltà di interrompere, modificare, prorogare, sospendere e revocare la procedura in qualsiasi momento, senza che ciò possa costituire, in alcun modo, diritto o pretesa a qualsivoglia risarcimento o indennizzo;

[1] Si invita L'operatore economico a non inviare informazioni che contengano informazioni e/o dati protetti da diritti di privativa o da diritti di proprietà intellettuale comunque rilevatori di segreti aziendali, commerciali, tecnici o industriali, ovvero di inviare, parallelamente alla presente dichiarazione, motivata e comprovata dichiarazione per la parte delle informazioni e/o documentazioni per le quali si richiede la non divulgazione.

E. di aver preso visione e di accettare il Codice Etico del Gruppo Ferrovie dello Stato Italiane, pubblicato al seguente indirizzo Internet: http://www.fsitaliane.it nella sezione "Il Gruppo FS" sottosezione "Governance" – sottosezione "Codice etico", di cui potrà chiedere in ogni momento copia cartacea, che è parte integrante del Modello di Organizzazione, Gestione e Controllo ex D.lgs. n. 231/2001 e s.m.i. di FS, di averne ben compreso i principi, i contenuti e le finalità e di obbligarsi al loro pieno ed integrale rispetto;

(a) di aver preso visione del Modello di Organizzazione, Gestione e Controllo ex D.lgs. n. 231/2001 e s.m.i. di FSTechnplogy ("Modello 231"), disponibile al seguente indirizzo Internet: http://www.fstechnology.it nella sezione "Chi siamo" sottosezione "Etica, compliance e integrità".

Il sottoscritto, in vista dell'eventuale accesso da parte di altri Operatori economici agli esiti della presente Consultazione, accetta espressamente che la divulgazione di quanto contenuto nei contributi forniti avverrà in forma anonima.

Il sottoscritto rende la presente dichiarazione sotto la propria responsabilità, consapevole delle sanzioni previste dalla legge a carico di chi attesta il falso e dichiara di essere informato che i dati personali raccolti saranno trattati in conformità con il Regolamento UE 2016/679, anche con strumenti informatici, esclusivamente nell'ambito del procedimento per il quale la presente dichiarazione viene resa.

A U T O R I Z Z A

Ferservizi SpA ad inviare le comunicazioni inerenti la presente procedura, ai contatti indicati al momento della registrazione sul Portale Acquisti Ferservizi, al sito www.acquistionlineferservizi.it

Luogo		Data	
Letto, confermato e sottoscritto			

*** NB: Le dichiarazioni dovranno essere firmate digitalmente dal legale rappresentante o procuratore munito di appositi poteri.**

TECHNOLOGY
GRUPPO FERROVIE DELLO STATO ITALIANE

Due Diligence
Questionario

ISTRUZIONI per la compilazione del Questionario di valutazione

Il questionario di valutazione ha l'obiettivo di valutare la copertura dei requisiti vincolanti e dei requisiti migliorativi ricompresi all'interno dell'RFI.
Di seguito si riportano le regole per la compilazione del Questionario:

> Da compilare la scheda "Riferimenti Operatore Economico".
All'Operatore Economico è richiesto di compilare la scheda "Riferimenti Operatore Economico", con tutti i riferimenti della persona responsabile di questa valutazione e rispondendo alle domande relative all'oggetto della presente consultazione di mercato.

> Da compilare la scheda "Requisiti vincolanti".
L'analisi dei requisiti vincolanti dell'Operatore Economico avviene come segue:
1:"Si" il requisito è soddisfatto dall'Operatore Economico.
2:"No" il requisito non è soddisfatto dall'Operatore Economico.
In assenza di risposta il requisito viene considerato non soddisfatto.
N.B. L'Operatore Economico che non abbia soddisfatto uno o più requisiti vincolanti sarà escluso dalla RFI.

> Da compilare la scheda "Requisiti migliorativi".
L'analisi dei requisiti migliorativi dell'Operatore Economico avviene:
a) con domanda chiusa, con risposta come segue:
1:"Si" il requisito è soddisfatto dall'Operatore Economico.
2:"No" il requisito non è soddisfatto dall'Operatore Economico.
In assenza di risposta il requisito viene considerato non soddisfatto.
b) con domanda aperta: in questo caso all'Operatore Economico è richiesto di compilare l'opportuno campo con le informazioni richieste, utili a valutare il soddisfacimento del requisito.
In assenza di risposta il requisito viene considerato non soddisfatto.

> La "POC" è una scheda consultiva, in cui vengono esplicitate le modalità di analisi del POC predisposto dall'Operatore Economico, che avverrà sulla base di specifici driver.

RIFERIMENTI OPERATORE ECONOMICO	RISPOSTA DELL'OPERATORE ECONOMICO
Ragione Sociale	
Codice Fiscale	
Nome e cognome del legale rappresentante che firma il questionario	

ID	DOMANDE RELATIVE ALL'OGGETTO DELLA PRESENTE CONSULTAZIONE DI MERCATO	RISPOSTA DELL'OPERATORE ECONOMICO
REF-01	*Fornire una breve descrizione dell'Operatore Economico (servizi offerti, certificazioni, appaltatori, ecc.)*	
REF-02	*Indicare l'esperienza maturata rispetto all'esigenza rappresentata nella presente consultazione di mercato o per iniziative analoghe*	
REF-03	*Numero totale di installazioni attive (funzionanti in ambienti di produzione) ad oggi. Per ogni installazione fornire i dettagli per l'Italia e/o l'Europa. Eventualmente, fornire una descrizione delle dimensioni/volumi (ad es. numero di utenti).*	
REF-04	*Descrivere eventuali alleanze, relazioni o dipendenze con terzi.*	
REF-05	*Fornire l'elenco di tutti i partner certificati (System Integrator/Consulting) ad oggi, che hanno prodotti certificati professionisti disponibili localmente.*	
REF-06	*Confermare la disponibilità locale di Ingegneri per l'erogazione di servizi di assistenza e per le fase di requisitazione/modellazione della soluzione proposta*	
REF-07	*Fornire informazioni dettagliate sui vostri tipi di formazione/corsi (materiali, durata, ecc.)*	
REF-08	*Fornire informazioni dettagliate sull'infrastruttura tecnica consigliata e sullo scenario di deployment dell'applicazione, compresi i requisiti minimi hardware, i requisiti tecnologici, i requisiti per la scalabilità e le prestazioni future, i requisiti di sicurezza dei dati e la protezione dei dati personali (caratteristiche GDPR).*	
REF-09	*Fornire informazioni sulla metodologia di implementazione suggerita*	
REF-10	*Presentare ulteriori informazioni/suggerimenti che possano essere utili per lo sviluppo di iniziative future.*	
REF-11	*Indicare il fatturato totale della società nell'ultimo triennio e la percentuale derivante dalla fornitura di prodotti e/o servizi simaliri a quelli oggetto della presente RFI*	

Tipologia Requisito	ID	Ambito	Descrizione	Copertura (Si/No)	Note
Requisiti di tipo funzionale	RF1	Data Entry	La piattaforma deve garantire l'inserimento dei seguenti dati concernenti l'operazione: - Tipologia operazione: Operazione straordinaria; adesione ad associazione; sponsorizzazione; partnership; co-marketing; consulenza; Altro (selezionabile da parte dell'utilizzatore tramite menù a tendina più campo "altro" per inserimento testo libero); - Area geografica/Paese: Il campo Area geografica/Paese potrà essere precompilata in automatico dalla piattaforma sulla base della localizzazione geografica dei soggetti sottoposti a verifiche; - Nominativo e ruolo controparti: I nominativi, oltre a essere aggiunti manualmente dall'utilizzatore, potranno essere precompilati in automatico dalla piattaforma sulla base di altri dati inseriti sui soggetti sottoposti a verifiche (es. partita IVA; analogo identificativo estero; identificativo in specifica banca dati); - Eventuali altre informazioni su campo libero.		
Requisiti di tipo funzionale	RF2	Data Entry	La piattaforma deve garantire l'inserimento dei seguenti dati concernenti i soggetti sottoposti a verifiche reputazionali (laddove applicabili, a seconda che si tratti di persone fisiche, persone giuridiche o altre entità: - Nome / Ragione o denominazione sociale - Data e luogo di costituzione / Data e luogo di nascita - Data e numero di iscrizione registro delle società - Sede Legale / Residenza - Sede Principale, degli affari (se Diversa dalla Sede Legale) / Domicilio (se diverso dalla residenza) - Partita IVA / Codice Fiscale - Area/e di attività - Forma legale - Numero di dipendenti - Ricavi annui ultimi 3 esercizi I dati di tale sezione dovranno essere, nella massima misura possibile, precompilati in automatico dalla piattaforma sulla base di altri dati inseriti sui soggetti sottoposti a verifiche (es. partita IVA; analogo identificativo estero; identificativo in specifica banca dati), ferma restando la possibilità di essere modificati/integrati manualmente dall'utilizzatore anche attraverso campi a testo libero.		
Requisiti di tipo funzionale	RF3	Schede	La piattaforma deve consentire la compilazione di moduli online, sia da parte di personale di altre società/strutture del Gruppo abilitate sia da parte di soggetti terzi		
Requisiti di tipo funzionale	RF4	Tracciatura Informazioni	Le operazioni a sistema devono essere tracciate, riconoscendo l'utente che le ha effettuate		
Requisiti di tipo funzionale	RF5	Notifiche	La piattaforma deve permettere l'invio di notifiche agli attori interessati al momento del caricamento dei documenti		
Requisiti di tipo funzionale	RF6	Note	La piattaforma deve permettere l'inserimento di note a corredo di ciascun documento caricato a sistema		
Requisiti di tipo funzionale	RF7	Data Retention	La piattaforma deve consentire una diversificazione dell'impostazione di data retention a seconda della tipologia della controparte		
Requisiti di tipo funzionale	RF8	Attivazione Due Diligence	La piattaforma deve permettere l' attivazione della Due Diligence tramite compilazione a sistema da parte della Struttura Richiedente di un form preliminare.		
Requisiti di tipo funzionale	RF9	Form preliminare	Il form preliminare, che innesca l'attività di Due Diligence deve poter essere customizzabile		
Requisiti di tipo funzionale	RF10	Pre-Scoring	Preliminarmente alla valutazione reputazionale, la piattaforma deve permettere l'attività di prescoring che consente un calcolo automatico sulla base di indicatori predeterminati, che possano essere configurati e/o suggeriti dalla piattaforma, quali ad esempio: - Livello di rischio del Paese di sede/residenza della terza parte e/o del Paese di riferimento dell'operazione; - Rischio del settore di attività della terza parte e/o settore di riferimento dell'operazione; - Elementi di complessità nella compagine della terza parte; - Presenza di altre red flags		
Requisiti di tipo funzionale	RF11	Analisi rischio	La piattaforma deve, in base alle risposte fornite nel form preliminare (Questionario Interno) assegnare un livello di rischio iniziale alla controparte (Alto, Medio, Basso), con possibilità di riclassificazione dell'esito della valutazione, corredata da un campo note		
Requisiti di tipo funzionale	RF12	Controlli differenziati	La piattaforma deve garantire l'implementazione di controlli differenziati in funzione del livello di rischio iniziale assegnato alla controparte		
Requisiti di tipo funzionale	RF13	Questionari esterni	La piattaforma deve permettere la somministrazione di questionari (questionari esterni) a terze parti		
Requisiti di tipo funzionale	RF14	Questionari esterni	La piattaforma deve consentire di inserire nei questionari sia domande a risposta chiusa che aperta.		
Requisiti di tipo funzionale	RF16	Questionari esterni	La piattaforma deve consentire di inserire nei questionari il controllo automatico di mancata compilazione dei campi, prevedendo campi obbligatori con alert in caso di mancato completamento.		
Requisiti di tipo funzionale	RF17	Accesso Terze parti	La piattaforma deve garantire l'accesso alle terze parti attraverso specifici meccanismi (es. con meccanismi di One Time Password).		
Requisiti di tipo funzionale	RF18	Allegati	La piattaforma deve garantire alla terza parte la possibilità di allegare la documentazione a corredo (es. Bilanci, Statuto, Atto Costitutivo, etc.)		
Requisiti di tipo funzionale	RF19	Canali comunicazione	La piattaforma deve garantire alla terza parte la possibilità di utilizzare l'area di chat per comunicare con la struttura richiedente		
Requisiti di tipo funzionale	RF20	Analisi rischio	L'analisi del rischio, effettuata automaticamente dalla piattaforma, deve tener conto di controlli standard		
Requisiti di tipo funzionale	RF21	Analisi rischio	L'analisi del rischio, effettuata automaticamente dalla piattaforma, deve tener conto di controlli aggiuntivi nel caso in cui il livello di rischio sia incrementato		
Requisiti di tipo funzionale	RF22	Analisi rischio	L'analisi del rischio, effettuata automaticamente dalla piattaforma, deve tener conto di rivalutazioni manuali del rischio		
Requisiti di tipo funzionale	RF23	Analisi rischio	L'analisi del rischio, effettuata automaticamente dalla piattaforma, deve verificare la presenza di eventuali Red Flag		
Requisiti di tipo funzionale	RF24	Analisi rischio	L'analisi del rischio, effettuata automaticamente dalla piattaforma, deve tener conto della definizione di un piano di mitigazione degli eventuali Red Flag		
Requisiti di tipo funzionale	RF25	Analisi rischio	La piattaforma, a valle dell'analisi del rischio, deve calcolare il rischio finale		
Requisiti di tipo funzionale	RF26	Analisi rischio	L'analisi del rischio, effettuata automaticamente dalla piattaforma, deve tener conto del profilo approvativo in base ai Red Flag e la piano di mitigazione		
Requisiti di tipo funzionale	RF27	Analisi sulla controparte	La piattaforma deve permettere l'analisi della controparte considerando la Ricostruzione degli assetti proprietari tramite recupero di informazioni da info-provider attraverso connettori		
Requisiti di tipo funzionale	RF28	Analisi sulla controparte	La piattaforma, nell'analisi della controparte, deve garantire il settaggio del valore soglia relativo alla percentuale di partecipazione proprietaria oltre la quale estendere i controlli sui soggetti		
Requisiti di tipo funzionale	RF29	Analisi sulla controparte	La piattaforma deve permettere la ricostruzione della struttura organizzativa tramite recupero di informazioni da info-provider attraverso connettori alle banche dati		
Requisiti di tipo funzionale	RF30	Analisi sulla controparte	La piattaforma deve garantire lo screening della terza parte e di tutti i soggetti individuati in base alle precedenti fasi di data entry e pre-due diligence (es. directors, shareholders, Ultimate Beneficial Owner, altri soggetti rilevanti immessi dall'utilizzatore della piattaforma), mediante l'interrogazione di infoprovider specializzati attualmente in uso (Bureau van Dijk, RDC On Board e Refinitiv World Check One, ferma restando la possibilità di integrare l'elenco degli infoprovider con ulteriori database di informazioni commerciali), che deve avvenire almeno sulle seguenti categorie di rischio: Adverse Media, Corruption, Sanctions list, Enforcement, Politically Exposed Persons (PEPs), State Owned Entity (SOE)		
Requisiti di tipo funzionale	RF31	Analisi sulla controparte	La piattaforma deve avere un connettore nativo con l'info-provider Dun & Bradstreet (controparti estere)		
Requisiti di tipo funzionale	RF32	Analisi sulla controparte	La piattaforma deve avere un connettore nativo con l'info-provider Bureau van Dijk (controparti italiane ed estere)		
Requisiti di tipo funzionale	RF33	Analisi sulla controparte	La piattaforma deve avere un connettore nativo con l'info-provider RDC on Board		
Requisiti di tipo funzionale	RF34	Analisi sulla controparte	La piattaforma deve avere un connettore nativo con l'info-provider Refinitiv World Check One		
Requisiti di tipo funzionale	RF35	Analisi sulla controparte	La piattaforma deve avere un connettore nativo con l'info-provider Cribis (controparti italiane)		
Requisiti di tipo funzionale	RF36	Visualizzazione Assetto	La piattaforma deve consentire la possibilità di visualizzazione grafica dell'assetto di controllo		
Requisiti di tipo funzionale	RF37	Visualizzazione Assetto	La piattaforma deve consentire la possibilità di visualizzare in forma tabellare l'assetto di controllo		
Requisiti di tipo funzionale	RF38	Red Flag	La piattaforma deve consentire la possibilità di evidenziare Red Flag nei casi di impossibilità di identificare il Beneficial Owner.		
Requisiti di tipo funzionale	RF39	Analisi reputazionale multi-sorgente	La piattaforma deve garantire l'esecuzione di verifiche su strutture proprietarie di controllo, nonchè Directors e Managers importando le informazioni derivate dall'info-provider. Tali dati dovranno essere, nella massima misura possibile, precompilati in automatico dalla piattaforma sulla base di altri dati inseriti sui soggetti sottoposti a verifiche (es. partita IVA; analogo identificativo estero; identificativo in specifica banca dati).		
Requisiti di tipo funzionale	RF40	Analisi reputazionale multi-sorgente	La piattaforma deve garantire la possibilità di inserire/modificare manualmente nominativi di soggetti per i quali è necessaria la verifica reputazionale, anche attraverso campi a testo libero		
Requisiti di tipo funzionale	RF41	Analisi reputazionale multi-sorgente	La piattaforma deve consentire l'esecuzione di ricerche sul web per trovare Adverse Media sulle singole entità identificate durante l'esecuzione dei controlli precedenti, dando evidenza di potenziali Red Flag e/o di eventuali falsi positivi		

Requisiti di tipo funzionale	RF42	*Analisi reputazionale multi-sorgente*	*La piattaforma deve consentire l'esecuzione di ricerche sul web in lingua italiana*		
Requisiti di tipo funzionale	RF43	*Analisi reputazionale multi-sorgente*	*La piattaforma deve consentire l'esecuzione di ricerche sul web in lingua inglese*		
Requisiti di tipo funzionale	RF46	*Report di Due Diligence*	*La piattaforma deve garantire la produzione e validazione del Report di Due Diligence*		
Requisiti di tipo funzionale	RF47	*Report di Due Diligence*	*Il Report prodotto dalla piattaforma deve riportare la valutazione finale del livello di rischio associato alla controparte*		
Requisiti di tipo funzionale	RF48	*Report di Due Diligence*	*Il Report prodotto dalla piattaforma deve riportare le evidenze dei Red Flags emersi nelle fasi precedenti*		
Requisiti di tipo funzionale	RF49	*Report di Due Diligence*	*Il Report prodotto dalla piattaforma deve permettere l'eventuale inserimento di proposte da parte di Compliance (da inserire in un campo note a testo libero) a mitigazione delle Red Flags identificate.*		
Requisiti di tipo funzionale	RF50	*Report di Due Diligence*	*La piattaforma deve essere in grado di archiviare i report (e l'eventuale documentazione allegata) secondo la data di ricerca/analisi al fine di garantire la storicizzazione dei dati.*		
Requisiti di tipo funzionale	RF51	*Validazione analisi reputazionale*	*Nella fase di validazione dell'analisi reputazione, la piattaforma deve consentire la modifica dei risultati delle interrogazioni, eliminando i risultati ritenuti c.d. "falsi positivi", anche secondo criteri di scrematura automatica dei falsi positivi, a condizione che delle corrispondenze scartate venga mantenuta evidenza e possano essere ripristinate a giudizio dell'utilizzatore della piattaforma.*		
Requisiti di tipo funzionale	RF52	*Validazione analisi reputazionale*	*Nella fase di validazione dell'analisi reputazione, la piattaforma deve consentire la modifica dei risultati delle interrogazioni, mitigando o innalzando manualmente livelli/elementi di rischio rilevati automaticamente dalla piattaforma stessa.*		
Requisiti di tipo funzionale	RF53	*Validazione analisi reputazionale*	*Nella fase di validazione dell'analisi reputazione, la piattaforma deve consentire la modifica dei risultati delle interrogazioni, aggiungendo note a testo libero e allegando documenti.*		
Requisiti di tipo funzionale	RF54	*Processo di Due Diligence*	*La piattaforma deve consentire, in tutte le fasi di processo, di inserire note e valutazioni delle risultanze della Due Diligence delle valutazioni dei Red Flags, nonché di allegare ulteriore documentazione (es. tratta da fonti esterne o Report di Due Diligence prodotti da fornitori specializzati)*		
Requisiti di tipo funzionale	RF55	*Processo di Due Diligence*	*La piattaforma deve gestire diversi livelli approvativi (tramite Workflow)*		
Requisiti di tipo funzionale	RF56	*Organigrammi*	*La piattaforma deve poter gestire gli organigrammi e le variazioni agli stessi*		
Requisiti di tipo funzionale	RF57	*Notifiche*	*La piattaforma deve inviare notifiche sulle attività pending*		
Requisiti di tipo funzionale	RF58	*Dashboard*	*Ciascun utente, nel momento in cui si collega al sistema, deve poter visualizzare una maschera riepilogativa delle attività a suo carico*		
Requisiti di tipo funzionale	RF59	*Report*	*La piattaforma deve predisporre Report sia in fase di avanzamento delle Due Diligence (stato di avanzamento, profilo di rischio, Red Flags emerse, workflow approvativi differenziati in caso di escalation) sia in fase di output (le informazioni raccolte nel processo di analisi, risk scoring, informazioni preliminari, evidenze di Red Flags, ecc.)*		
Requisiti di tipo funzionale	RF60	*Ricerca*	*La piattaforma deve consentire la ricerca full text nelle sezioni*		
Requisiti di tipo funzionale	RF61	*Ricerca*	*La piattaforma deve consentire la ricerca full text nei documenti allegati*		
Requisiti di tipo funzionale	RF62	*Export informazioni*	*La piattaforma deve consentire l'export delle informazioni presenti in piattaforma sui principali formati file della Suite Office)*		
Requisiti di tipo funzionale	RF63	*Export informazioni*	*La piattaforma deve consentire l'export delle informazioni presenti in piattaforma in formato PDF*		
Requisiti di tipo funzionale	RF64	*Reporting*	*La piattaforma deve predisporre reporting tramite cruscotti dedicati*		
Requisiti di tipo tecnico	RT1	*SaaS Platform*	*La piattaforma deve essere deliverata in modalità SaaS (Software as a Service).*		
Requisiti di tipo tecnico	RT2	*Web-based app*	*La piattaforma deve essere web based ovvero accessibile da web.*		
Requisiti di tipo tecnico	RT3	*Responsive*	*La Piattaforma deve essere responsive, in modo che si possa visualizzare e usufruire da ogni browser, device (cellulare, computer, tablet, etc.) e sistema operativo e browser. In particolare, da Mobile per Android a partire dalla versione 6.0 in poi - IOS da versione IOS 10 in poi.*		
Requisiti di tipo tecnico	RT4	*Accesso alla piattaforma per i dipendenti del Gruppo FS*	*I dipendenti del Gruppo FS devono essere autenticati e autorizzati sulla piattaforma con supporto del protocollo Azure Active Directory*		
Requisiti di tipo tecnico	RT5	*Profilazione*	*La piattaforma deve permettere di definire dei ruoli e di profilare gli utenti in modo da gestire i coni di visibilità ed i permessi sulla base di specifici parametri ed esigenze (es. società, struttura organizzativa, ecc.).*		
Requisiti di tipo tecnico	RT6	*Scalabilità*	*La piattaforma deve essere scalabile e permettere di aggiungere maggiori risorse con l'obiettivo di supportare un numero crescente di utenti, società, documenti e dati in generale rispetto alla baseline.*		
Requisiti di tipo tecnico	RT7	*Compatibilità a fronte di nuove realease della piattaforma*	*L'Operatore Economico deve assicurare, a fronte di rilasci di nuove versioni principali o secondarie della piattaforma (major/minor release), la compatibilità con tutte le configurazioni/personalizzazioni effettuate per rispondere all'esigenze dell'organizzazione, nonché la compatibilità con le integrazioni attivate con i sistemi del Gruppo FS. Inoltre, l'Operatore Economico deve descrivere, mediante documentazione opportuna, il processo e le modalità di aggiornamento dell'applicazione SaaS, indicando in maniera trasparente e chiara l'impatto di ogni operazione sulle funzionalità del servizio. L'Operatore Economico deve condividere il piano e le modalità di test end to end delle modifiche apportate.*		
Requisiti di tipo tecnico	RT8	*Integrazione via Web Services*	*La piattaforma deve consentire l'integrazione con altri servizi tramite Web Services e API.*		
Requisiti di tipo tecnico	RT9	*Integrazione con altri sistemi aziendali*	*La piattaforma deve consentire l'integrazione con la suite Microsoft Office365.*		
Requisiti di tipo tecnico	RT10	*Integrazione con altri sistemi aziendali*	*La piattaforma deve consentire l'integrazione Sharepoint.*		
Requisiti di tipo tecnico	RT11	*Integrazione con altri sistemi aziendali*	*La piattaforma deve consentire l'integrazione con altri sistemi aziendali: es. SAP BW/4, SAP S/4, SAP Ecc, SAP BW Netweaver, SAP HR.*		
Requisiti di tipo tecnico	RT12	*Integrazione con altri sistemi aziendali*	*Il sistema deve consentire l'integrazione con la piattaforma Oracle Enterprise Performance Management.*		
Requisiti di tipo tecnico	RT13	*Estrazione completa dei dati*	*Deve essere sempre possibile da parte di FS Technology, l'estrazione di una copia completa dei dati memorizzati e gestiti dal servizio (in formato standard, non proprietario e riutilizzabile), ivi compresi i dati derivati quali log e statistiche di utilizzo, nonché le configurazioni del servizio.*		
Requisiti di tipo tecnico	RT14	*Migrazione verso altra applicazione*	*Al termine del contratto, deve essere prevista un'attività di migrazione dei dati del servizio verso un'altra applicazione con conseguente eliminazione permanente dei dati di proprietà del Gruppo FS al termine della procedura di migrazione (inclusi i dati derivati e i dati di backup). Per quanto riguarda i documenti, i file dovranno essere esportati in formato originale, o in altro formato standard di mercato, secondo quanto indicato dal Committente. Dovrà essere fornita dettagliata ed esaustiva documentazione delle modalità di indicizzazione e di archiviazione dei documenti (metadati, IdC, etc.) per consentire un'agevole presa in carico dei documenti restituiti.*		
Requisiti di tipo tecnico	RT15	*Ambienti*	*Il servizio deve consentire la separazione degli ambienti in sviluppo, certificazione e produzione, con il rispetto dei passaggi previsti per favorire l'esecuzione delle attività di sviluppo e testing in modo controllato e sicuro (non prevedendo l'utilizo di dati reali in ambienti di test e sviluppo).*		
Requisiti di tipo tecnico	RT16	*Utenze di test*	*L'Operatore Economico SaaS deve rendere disponibile un account di test per ogni ruolo ed un URL utilizzabili dall'acquirente per effettuare ogni tipo di verifica necessaria per il rilascio di nuove evolutive.*		
Requisiti di tipo tecnico	RT17	*Change Management*	*Adozione di procedure/strumenti di change management per tenere traccia delle modifiche eseguite sulle configurazioni del sistema.*		
Requisiti di tipo tecnico	RT18	*Personalizzazione/configurazione interfaccia*	*Il sistema gode di flessibilità sufficiente per l'adattamento dei form e la configurazione dell'interfaccia rispetto alle specifiche funzionali e di layout previste in fase di progettazione.*		
Requisiti di tipo tecnico	RT19	*Creazione reportistica*	*Il sistema dovrà essere in grado di produrre Report predefiniti standard e custom in formato Word, Pdf, Power Point ed Excel.*		
Requisiti di supporto e manutenzione	S1	*Presenza in Italia*	*L'Operatore Economico deve avere sedi in Italia in grado di erogare supporto.*		
Requisiti di supporto e manutenzione	S2	*Supporto tecnico e supporto operativo agli Utenti FSTechnology gestori*	*È richiesto all'Operatore Economico di erogare supporto tecnico e supporto operativo agli utenti FSTechnology gestori della piattaforma per tutta la durata del contratto.*		
Requisiti di supporto e manutenzione	S3	*Supporto tecnico e supporto operativo agli Utenti finali*	*È richiesta all'Operatore Economico di erogare supporto tecnico e supporto operativo agli utenti finali per l'utilizzo della piattaforma per tutta la durata del contratto.*		
Requisiti di supporto e manutenzione	S4	*Canali di supporto base*	*L'Operatore Economico deve garantire il supporto al Gruppo FS attraverso i seguenti canali: e-mail.*		
Requisiti di supporto e manutenzione	S5	*Canali di supporto base*	*L'Operatore Economico deve garantire il supporto al Gruppo FS attraverso un canale ticketing.*		
Requisiti di supporto e manutenzione	S8	*Sistema di trouble ticketing*	*L'Operatore Economico deve allestire un sistema di trouble ticketing di tipo web-based, per la raccolta e la piena condivisione a FSTechnology delle difformità e dei disservizi riscontrati durante l'esercizio. In particolare, il sistema deve consentire:* *- il monitoraggio in maniera autonoma dei ticket aperti e del loro stato di elaborazione;* *- la generazione di reportistica relativa all'insieme di ticket aperti in un determinato periodo di riferimento.*		

Requisiti di supporto e manutenzione	S10	*Orari supporto minimo*	*Il supporto deve essere garantito: - 5 giorni alla settimana lavorativi secondo il calendario italiano; - orario 8-18 nei giorni lavorativi del calendario italiano.*		
Requisiti di supporto e manutenzione	S12	*Lingua supporto*	*Il supporto dell'Operatore Economico deve essere in Lingua Italiana.*		
Requisiti di supporto e manutenzione	S14	*Recovery Time Objective (RTO)*	*Recovery Time Objective (RTO, inteso come il massimo tempo di indisponibilità del servizio) pari a 4 ore. Formula per il calcolo NRTO = numero di eventi di fermo con mancato rispetto del RTO Periodo di riferimento per il calcolo: mensile.*		
Requisiti di supporto e manutenzione	S15	*Disponibilità del servizio*	*Disponibilità del servizio su base mensile pari ad almeno il 98% delle ore totali (nel calcolo della disponibilità del servizio non saranno considerate interruzioni dovute a eventi di forza maggiore, inteso come un evento al di fuori del controllo dell'Operatore Economico o dovute a interventi manutentivi).*		
Requisiti di supporto e manutenzione	S16	*Tempo di presa in carico*	*Tempo di presa in carico pari a 4 ore negli orari del supporto dalla segnalazione/richiesta di intervento.*		
Requisiti di supporto e manutenzione	S17	*Tempo di risoluzione del malfunzionamento in caso di errori bloccanti*	*Tempo di risoluzione del malfunzionamento in caso di errori bloccanti pari a 12 ore dalla presa in carico.*		
Requisiti di supporto e manutenzione	S18	*Risoluzione malfunzionamenti non bloccanti*	*Tempo di risoluzione del malfunzionamento non bloccante entro massimo 36 ore dalla presa in carico.*		
Requisiti di Sicurezza e Cyber	C.O.1	*Ruoli e Responsabilità definiti formalmente in ambito Data Protection*	Identificazione dei ruoli e delle responsabilità associate alle persone coinvolte nel trattamento dei dati		
Requisiti di Sicurezza e Cyber	C.O.2	*Formazione periodica in ambito Data Protection*	*Esistenza di corsi in aula o E-learning, newsletter, pillole formative periodiche per accrescere la conoscenza delle tematiche relative alla Data Protection*		
Requisiti di Sicurezza e Cyber	C.O.3/9	*Svolgimento audit di sicurezza periodici e verifica in materia Data Protection*	*Esistenza di un processo periodico relativo all'esecuzione di audit di sicurezza, incluso la verifica della conformità normativa in ambito Data Protection*		
Requisiti di Sicurezza e Cyber	C.O.4	*Monitoraggio periodico delle non conformità normative in ambito Data Protection*	*Esistenza di un processo periodico di monitoraggio delle non conformità normative rilevate nei precedenti audit*		
Requisiti di Sicurezza e Cyber	C.O.5	*Policy di sicurezza*	*Esistenza di politiche di sicurezza delle informazioni dell'intera organizzazione*		
Requisiti di Sicurezza e Cyber	C.O.6	*Modello di controlli IT*	*Definizione di un set di controlli IT da implementare basati sui principali standard*		
Requisiti di Sicurezza e Cyber	C.O.7	*Certificazione del sistema di sicurezza*	*Verifica di un sistema per l'acquisizione di un certificato che attesti che quel dato sistema soddisfa i requisiti di sicurezza dettati dall'entità certificatrice*		
Requisiti di Sicurezza e Cyber	C.O.8	*Risk Assessment periodici*	*Devono essere periodicamente (almeno annualmente) effettuate delle sessioni di analisi, valutazione e trattamento dei rischi.*		
Requisiti di Sicurezza e Cyber	C.O.9	*Implementazione inventario HW/SW*	*Implementare un inventario dei dispositivi hardware e del software di proprietà dell'organizzazione.*		
Requisiti di Sicurezza e Cyber	C.O.10	*Policy per la gestione degli accessi ai sistemi informatici*	*Esistenza di politiche per la gestione degli accessi ai sistemi informatici*		
Requisiti di Sicurezza e Cyber	C.O.11	*Review periodica delle utenze*	*Esistenza di un processo di revisione periodica delle utenze profilate nei sistemi*		
Requisiti di Sicurezza e Cyber	C.O.12	*Policy per la gestione del ciclo di vita del software (Secure SDLC)*	*Esistenza di una politica che definisce un ciclo di sviluppo sicuro del software secondo gli attuali standard di settore (es. OWASP)*		
Requisiti di Sicurezza e Cyber	C.O.13	*Formazione sullo sviluppo sicuro*	*Assicurare che il personale che sviluppa abbia ricevuto un'adeguata formazione sulla scrittura di codice sicuro nel loro specifico ambiente di sviluppo.*		
Requisiti di Sicurezza e Cyber	C.O.14	*Policy per la gestione degli incidenti di sicurezza*	*Esistenza di politiche di gestione degli incidenti di sicurezza*		
Requisiti di Sicurezza e Cyber	C.O.15	*Istruzioni operative per l'utilizzo delle risorse informatiche e internet*	*Definizione e implementazione di istruzioni operative per l'utilizzo delle risorse informatiche e internet*		
Requisiti di Sicurezza e Cyber	C.O.16	*Istruzioni operative per la cancellazione sicura dei dispositivi*	*Esistenza di una procedura che preveda la possibilità di cancellare in modo sicuro i dati dai dispositivi che trattano dati personali*		
Requisiti di Sicurezza e Cyber	C.O.17/18	*Clausola contrattuali, SLA e processo di monitoraggio dell'operato delle Terze Parti o "persone correlate"*	*Definizione degli indicatori di prestazione chiave tra il Responsabile e le "persone correlate" ad esso, al fine di fornire il livello di servizio desiderato e di revisionare periodicamente l'operato delle persone correlate.*		
Requisiti di Sicurezza e Cyber	C.O.18	*Reputation e Data Breach*	*E' necessario definire ed implementare un processo per tutelare la presenza sul web dell'organizzazione. In particolar modo identificare siti illegittimi e monitorare il web per identificare potenziali data breach.*		
Requisiti di Sicurezza e Cyber	C.O.19	*Misure prescrittive per amministratori di sistema*	*Esistenza di specifiche misure di sicurezza che devono essere adottate dagli amministratori di sistema*		
Requisiti di Sicurezza e Cyber	C.O.21	*Backup - Definizione policy*	*Deve essere definita ed implementata una opportuna policy per la gestione del backup.*		
Requisiti di Sicurezza e Cyber	C.O.22	*Public Key Infrastructure - Processo di gestione chiavi di cifratura*	*Deve essere definito e documentato un processo per la gestione del ciclo di vita delle chiavi di cifratura / mascheramento dati (creazione, archiviazione, recupero, distribuzione, ritiro e distruzione).*		
Requisiti di Sicurezza e Cyber	C.O.23	*Public Key Infrastructure - Nomina dei responsabili delle chiavi di cifratura*	*Devono essere nominati i responsabili delle chiavi di cifratura / mascheramento dati e sensibilizzati sulle proprie responsabilità nell'uso e protezione delle chiavi.*		
Requisiti di Sicurezza e Cyber	C.O.24	*Ruoli e responsabilità in ambiente cloud*	*Devono essere definiti, registrati e comunicati in modo chiaro i ruoli e le responsabilità (in condivisione o suddivisione) in carico all'organizzazione e al Cloud Provider.*		
Requisiti di Sicurezza e Cyber	C.O.26	*Localizzazione dei Data Center*	*I datacenter e le informazioni/servizi in Cloud devono risiedere su territorio nazionale o all'interno dell'Unione Europea*		
Requisiti di Sicurezza e Cyber	C.O.27	*Notifica data breach da parte del Cloud Provider*	*Il Cloud Provider deve segnalare tempestivamente all'organizzazione eventuali accessi non autorizzati a dati soggetti a regolamento GDPR, che possano causare perdite, divulgazioni o alterazioni dei dati.*		
Requisiti di Sicurezza e Cyber	C.O.28	*Accordi di non divulgazione (Non Disclosure Agreement, NDA)*	*Il personale del Cloud Provider avente accesso a dati riservati deve essere soggetto ad obblighi di riservatezza*		
Requisiti di Sicurezza e Cyber	C.O.31	*Processo formale di Change & Patch management*	*Definizione di un processo formale che documenti la fase di autorizzazione e implementazione delle modifiche e dell'installazione delle patch all'interno di processi, sistemi o strutture aziendali*		

Requisiti di Sicurezza e Cyber	C.T.1	*Meccanismi di identificazione e autenticazione*	*Esistenza di meccanismi di accesso ai sistemi tramite il riconoscimento attraverso un nome utente e l'autenticazione attraverso password.*		
Requisiti di Sicurezza e Cyber	C.T.2	*Utilizzo utenze univoche e nominali*	*Esistenza di utenze che siano associate in modo univoco a persone fisiche, identificabili con nome e cognome e/o riconducibili univocamente ad un unico soggetto responsabile*		
Requisiti di Sicurezza e Cyber	C.T.3	*Meccanismi di autorizzazione*	*Implementazione di controlli che permettano di definire quali operazioni possa compiere una specifico utente*		
Requisiti di Sicurezza e Cyber	C.T.4	*Gestione utenze Privilegiate*	*Implementazione di controlli specifici sulle utenze con privilegi ampi per impedire operazioni illecite*		
Requisiti di Sicurezza e Cyber	C.T.5	*Password policy conforme alle linee guida aziendali*	*Insieme di regole che definiscono come dovrebbe essere costituita una password affinché possa essere ritenuta sufficientemente sicura; tale misura è associata alle utenze interne (non clienti).*		
Requisiti di Sicurezza e Cyber	C.T.6	*Strong Authentication*	*Esistenza di un sistema di autenticazione forte a a 2 fattori (es. password + one time password)*		
Requisiti di Sicurezza e Cyber	C.T.7	*Accesso logico terze parti*	*L'accesso logico ai sistemi da parte di terzi (ad esempio clienti, fornitori, consulenti) deve essere soggetto a controlli rigorosi.*		
Requisiti di Sicurezza e Cyber	C.T.8	*Tracciamenti accessi utenti*	*Registrazione e memorizzazione dei log degli accessi degli utenti (es. login, logout e principali attività utente, ad esempio download di dati, cancellazione di dati, modifiche massive dei dati)*		
Requisiti di Sicurezza e Cyber	C.T.9	*Tracciamento accessi Amministratori di Sistema*	*Registrazione e memorizzazione dei log degli accessi degli Amministratori di Sistema (es. login, logout e principali attività utente, ad esempio download di dati, cancellazione di dati, modifiche massive dei dati)*		
Requisiti di Sicurezza e Cyber	C.T.10	*Protezione dei log*	*Esistenza di meccanismi di protezione dei log in maniera da non poter essere cancellati da personale non autorizzato.*		
Requisiti di Sicurezza e Cyber	C.T.11	*Retention dei log*	*Esistenza di un limite temporale entro il quale possano essere conservati i log*		
Requisiti di Sicurezza e Cyber	C.T.12	*Tracciamento degli Incident*	*Registrazione e memorizzazione degli incidenti avvenuti/individuati*		
Requisiti di Sicurezza e Cyber	C.T.13	*Network Time Protocol (NTP)*	*Configurazione del protocollo NTP al fine di sincronizzare il clock del sistema*		
Requisiti di Sicurezza e Cyber	C.T.14	*Monitoraggio delle performance*	*Attività di monitoraggio delle performance del sistema in modo da verificare che siano rispettati i livelli di servizio stabiliti*		
Requisiti di Sicurezza e Cyber	C.T.15	*Invio Log a piattaforma di analisi e correlazione eventi (es: SIEM, CASB)*	*Reindirizzamento dei log dei vari sistemi all'interno di un sistema centralizzato che si occupa della correlazione degli eventi e dell'analisi di eventuali anomalie*		
Requisiti di Sicurezza e Cyber	C.T.16/17	*Sistema monitorato da SOC h24*	*Sistema soggetto a monitoraggio real time 24 ore su 24 da parte di un centro altamente specializzato nell'individuazione di eventuali anomalie nei sistemi e nelle reti*		
Requisiti di Sicurezza e Cyber	C.T.18	*Cifratura dei canali di trasmissione (HTTPS)*	*Esistenza di tecniche e protocolli per la protezione dei dati durante le transazioni (es. https)*		
Requisiti di Sicurezza e Cyber	C.T.19/20	*Hardening dei sistemi*	*Implementazione di specifiche configurazioni su sistemi e componenti che permettono di incrementare la sicurezza di un sistema.*		
Requisiti di Sicurezza e Cyber	C.T.21	*Strumenti e Metodologie di Threat Intelligence*	*Deve essere definito e implementato un processo di Threat Intelligence, per raccogliere, analizzare ed elaborare le informazioni relative alle potenziali minacce che possono impattare l'organizzazione e appositi strumenti e data feed*		
Requisiti di Sicurezza e Cyber	C.T.22	*Host Intrusion Detection System (HIDS)*	*Utilizzo di Host Intrustion Detection System*		
Requisiti di Sicurezza e Cyber	C.T.23	*Host Intrusion Prevention System (HIPS)*	*Utilizzo di Host Intrustion Prevention System*		
Requisiti di Sicurezza e Cyber	C.T.24	*Antivirus*	*Adozione di strumenti di prevenzione e protezione da virus.*		
Requisiti di Sicurezza e Cyber	C.T.25	*Anti-malware*	*Adozione di strumenti di prevenzione e protezione da malware.*		
Requisiti di Sicurezza e Cyber	C.T.26	*Collezionamento eventi virus su piattaforma centralizzata*	*Tutti gli eventi virus-related devono essere inviati ad una piattaforma centralizzata di collezionamento.*		
Requisiti di Sicurezza e Cyber	C.T.27	*Collezionamento eventi malware su piattaforma centralizzata*	*Tutti gli eventi malware-related devono essere inviati ad una piattaforma centralizzata di collezionamento.*		
Requisiti di Sicurezza e Cyber	C.T.28	*Aggiornamento software anti-virus*	*Il software anti-virus deve essere costantemente aggiornato.*		
Requisiti di Sicurezza e Cyber	C.T.29	*Aggiornamento software anti-malware*	*Il software anti-malware deve essere costantemente aggiornato.*		
Requisiti di Sicurezza e Cyber	C.T.30/31	*Patch Management*	*Installazione di patch di sicurezza sui sistemi per risolvere le vulnerabilità rilevate*		
Requisiti di Sicurezza e Cyber	C.T.32	*Patch Management tramite tool automatici*	*Utilizzo di tool automatici per le attività di patch management.*		
Requisiti di Sicurezza e Cyber	C.T.33	*Vulnerability Assessment*	*Attività periodiche schedulate ed effettuate da sonde in grado di rilevare vulnerabilità sui sistemi operativi ed applicativi.*		
Requisiti di Sicurezza e Cyber	C.T.34	*Penetration Test*	*Attività di analisi di sicurezza mirate, con lo scopo di rilevare vulnerabilità e simulare attacchi informatici*		
Requisiti di Sicurezza e Cyber	C.T.35	*Simulazione Red Team vs Blue Team*	*Effettuare periodicamente simulazioni di attacco per testare il livello di efficacia dell'organizzazione nel reagire.*		
Requisiti di Sicurezza e Cyber	C.T.36	*Back up periodico*	*Effettuazione pianificata di copie di riserva finalizzata a duplicare, con una periodicità prestabilita, i dati, le configurazioni e le immagini di sistema su appositi supporti di memorizzazione.*		
Requisiti di Sicurezza e Cyber	C.T.37	*Disaster recovery*	*Definizione di procedure per garantire la possibilità di mantenere in piedi un servizio/sistema anche in caso di malfunzionamento, sia di natura accidentale che malevola, e di poter ristabilire in tempi definiti l'operatività completa dei sistemi (è richiesto un piano di Disaster recovery).*		
Requisiti di Sicurezza e Cyber	C.T.38	*Piani di continuità operativa*	*Definizione di procedure per garantire la possibilità di mantenere in piedi un servizio/sistema anche in caso di malfunzionamento, sia di natura accidentale che malevola, e di poter ristabilire in tempi definiti l'operatività completa dei sistemi (è richiesto un piano di Continuità operativa).*		
Requisiti di Sicurezza e Cyber	C.T.39	*High Availability*	*Implementazione di un modello che permette, tramite l'adozione di strumenti tecnologici ridondati, di avere un sistema altamente disponibile ai propri utenti.*		
Requisiti di Sicurezza e Cyber	C.T.40	*Test periodici*	*Implementare periodicamente dei test di ripristino delle copie di backup.*		
Requisiti di Sicurezza e Cyber	C.T.41	*Protezione copie di backup*	*Le copie di backup devono essere protette mediante opportune misure di sicurezza fisica e logica (protezione da perdite, danni e accessi non autorizzati).*		
Requisiti di Sicurezza e Cyber	C.T.42	*Cifratura copie di backup*	*Le copie di backup devono essere protette mediante opportune misure di sicurezza fisica e logica (tramite cifratura dati).*		
Requisiti di Sicurezza e Cyber	C.T.43	*Tecniche di cifratura*	*Esistenza di tecniche di cifratura dei dati memorizzati (es. dati memorizzati nei database o nelle memorie di massa)*		
Requisiti di Sicurezza e Cyber	C.T.44	*Mascheramento dei dati*	*Esistenza di tecniche di data masking per minimizzare la visualizzazione e lettura di dati personali basati sul principio del "need to know"*		
Requisiti di Sicurezza e Cyber	C.T.45/46	*Segregazione ambienti*	*Separazione fisica o virtuale degli ambienti che compongono il sistema (es. sviluppo, test, formazione, produzione)*		
Requisiti di Sicurezza e Cyber	C.T.47	*Requisiti di sicurezza software fornitori*	*I fornitori di software devono garantire un adeguato livello di sicurezza del proprio software.*		
Requisiti di Sicurezza e Cyber	C.T.48	*Test su nuovi sistemi*	*I nuovi sistemi devono essere testati rigorosamente, in accordo con piani di test predefiniti e documentati, e i risultati approvati e firmati, prima dell'installazione in ambiente di esercizio.*		
Requisiti di Sicurezza e Cyber	C.T.49	*Controllo Accessi Fisici*	*Misure di sicurezza per controllare gli accessi che vengono effettuati al data center che ospita le macchine dell'organizzazione*		
Requisiti di Sicurezza e Cyber	C.T.50	*Antincendio*	*Misure di sicurezza per prevenire o far fronte ad un possibile incendio del Data Center che ospita le macchine dell'organizzazione*		
Requisiti di Sicurezza e Cyber	C.T.51	*Antiallagamento*	*Misure di sicurezza per prevenire o far fronte ad un possibile allagamento del Data Center che ospita le macchine dell'organizzazione.*		
Requisiti di Sicurezza e Cyber	C.T.52	*Controllo temperatura data center*	*Attività di monitoraggio della temperatura interna dei Data Center per tutelare le macchine in esso presenti.*		
Requisiti di Sicurezza e Cyber	C.T.53	*Sicurezza fisica dispositivi di rete*	*I cavi di rete ed i punti di accesso alla rete devono essere protetti mediante controlli fisici.*		
Requisiti di Sicurezza e Cyber	C.T.54	*Sicurezza fisica degli edifici*	*Gli edifici che ospitano l'infrastruttura IT dell'organizzazione devono essere fisicamente protetti contro incidenti o attacchi di sicurezza.*		
Requisiti di Sicurezza e Cyber	C.T.55	*Protezione da sbalzi/interruzioni di corrente*	*Le infrastrutture IT devono essere protette contro sbalzi o interruzioni di corrente.*		
Requisiti di Sicurezza e Cyber	C.T.56	*Input validation*	*Misure di sicurezza che rafforzano l'applicativo impedendo la possibilità di sfruttare vulnerabilità comuni (e.g. validazione degli input).*		
Requisiti di Sicurezza e Cyber	C.T.57	*Code review*	*È necessario eseguire dei controlli sul codice applicativo per identificare e indirizzare le vulnerabilità di sicurezza (ad esempio mediante analisi statica e dinamica del codice sorgente e test di unità).*		

Requisiti di Sicurezza e Cyber	C.T.59	*File Integrity Tool*	*Devono essere utilizzati opportuni strumenti di verifica dell'integrità dei file per assicurare che i file critici di sistema (compresi eseguibili, librerie e file di configurazione) non siano stati alterati.*		
Requisiti di Sicurezza e Cyber	C.T.60	*Protezione Avanzata Database*	*Le basi di dati contenenti informazioni e dati rilevanti devono essere protette contro l'accesso e la modifica non autorizzati.*		
Requisiti di Sicurezza e Cyber	C.T.66	*Cancellazione base (a livello software)*	*Utilizzo di algoritmi e meccanismi generici per la cancellazione dei dati*		
Requisiti di Sicurezza e Cyber	C.T.67	*Decommissioning e cancellazione sicura (a livello hardware)*	*Attività di dismissione sicura dei dispositivi di archiviazione utilizzati dai sistemi dell'organizzazione.*		
Requisiti di Sicurezza e Cyber	C.C.1	*Web Application Firewall (WAF)*	*Utilizzo di Web Application Firewall per la protezione dei sistemi*		
Requisiti di Sicurezza e Cyber	C.C.2	*Cifratura dei canali di trasmissione (es: VPN)*	*Esistenza di tecniche e protocolli per la protezione dei dati durante le transazioni (es. VPN)*		
Requisiti di Sicurezza e Cyber	C.C.3	*Protezione Anti DDOS*	*Esistenza di sistemi per la protezione da attacchi aventi come obiettivo l'indisponibilità di uno o più servizi*		
Requisiti di Sicurezza e Cyber	C.C.4	*Firewall*	*Il traffico di rete in ingresso e in uscita dalla rete dell'organizzazione deve essere instradato attraverso un firewall opportunamente configurato e gestito, al fine di bloccare, limitare e monitorare in maniera puntuale, il traffico in transito sulla rete.*		
Requisiti di Sicurezza e Cyber	C.C.5	*Rilevamento intrusioni sulla rete (NIDS)*	*Soluzioni di rilevamento delle intrusioni devono essere applicate alla rete dell'organizzazione.*		
Requisiti di Sicurezza e Cyber	C.C.6	*Network Intrusion Prevention System (NIPS)*	*Soluzioni di prevenzione delle intrusioni devono essere applicate alla rete dell'organizzazione.*		
Requisiti di Sicurezza e Cyber	C.C.7	*Controllo accessi alla rete mediante dispositivi mobili*	*L'accesso alla rete dell'organizzazione attraverso dispositivi mobili deve essere ristretto utilizzando tecnologie di Network Access Control (NAC), in grado di verificare la configurazione del dispositivo e gestire opportunamente l'accesso.*		
Requisiti di Sicurezza e Cyber	C.C.8	*Hardening dei dispositivi di rete*	*I dispositivi di rete devono essere hardenizzati e configurati in maniera sicura*		
Requisiti di Sicurezza e Cyber	C.C.10	*Network Level Authentication*	*Implementare l'autenticazione a livello rete mediante 802.1X al fine di limitare e controllare quali dispositivi possono accedere alla rete.*		
Requisiti di Sicurezza e Cyber	C.C.11	*IP Tracking*	*Associazione IP/Host/Hostname per identificazione dei dispositivi in rete (necessario per Data Breach Management)*		
Requisiti di Sicurezza e Cyber	C.C.12	*DNS Protection*	*Protezione dei server DNS per garantire la disponibilità della risoluzione dei nomi e quindi la possibilità di raggiungere l'applicazione*		
Requisiti di Sicurezza e Cyber	C.C.13	*Zero Trust*	*Adozione di un modello di sicurezza "Zero Trust"*		

Tipologia Requisito	ID	Titolo	Descrizione	Copertura (Si/No)	Note
Requisiti di tipo funzionale	RF44	*Analisi reputazionale multi-sorgente*	*La piattaforma consente l'esecuzione di ricerche sul web in lingua francese*		
Requisiti di tipo funzionale	RF45	*Analisi reputazionale multi-sorgente*	*La piattaforma consente l'esecuzione di ricerche sul web in lingua spagnola*		
Requisiti di tipo funzionale	RF65	*Alert*	*La piattaforma permette la ricezione di eventuali alert trasmessi tramite le funzionalità di monitoraggio continuo disponibili sulle banche dati, fornita da infoprovider esterni tramite API.*		
Requisiti di tipo funzionale	RF66	*Due Diligence precedenti*	*La piattaforma permette di attualizzare le Due Diligence svolte in passato*		
Requisiti di tipo funzionale	RF67	*Collegamento a Due Diligence precedenti*	*La piattaforma consente di creare collegamenti/link con Report di Due Diligence già concluse*		
Requisiti di tipo tecnico	RT20	*Integrazione con altri sistemi aziendali*	*La piattaforma consente l'integrazione con la piattaforma Salesforce*		
Requisiti di supporto e manutenzione	S6	*Canali di supporto extra*	*L'Operatore Economico garantisce il supporto al Gruppo FS attraverso un canale telefonico.*		
Requisiti di supporto e manutenzione	S7	*Canali di supporto extra*	*L'Operatore Economico garantisce il supporto al Gruppo FS attraverso un canale live chat*		
Requisiti di supporto e manutenzione	S9	*Integrazione canale di supporto ticketing*	*L'Operatore Economico supporta FSTechnology attraverso un canale ticketing integrabile con i sistemi di governance IT. Per garantire l'interoperabilità, occorre disporre di un web service di tipo SOAP o REST*		
Requisiti di supporto e manutenzione	S11	*Orari supporto*	*Il supporto è garantito:* *- 7/7 giorni alla settimana secondo il calendario italiano;* *- 24 ore su 24 nei giorni lavorativi del calendario italiano.*		
Requisiti di supporto e manutenzione	S13	*Lingua supporto*	*Il supporto dell'Operatore Economico è disponibile anche in Lingua Inglese.*		

Tipologia Requisito	ID	Titolo	Descrizione	Descrizione della funzionalità offerta dalla piattaforma (risposta operatore economico)
Requisiti di tipo funzionale	RF15	*Questionari esterni*	*A seguito della compilazione del Questionario da una Terza Parte, la piattaforma garantisce una modalità che permette di certificare l'autenticità del compilatore*	

Allegato 1.2

Progetto DIGITAL DUE DILIGENCE

Use Case

TECHNOLOGY
GRUPPO FERROVIE DELLO STATO ITALIANE

Introduzione

Progetto Digital Due Diligence – Introduzione

Si riportano alcune note utili per l'utilizzo del documento e relativa esecuzione del PoC:

- Viene fornita la partita IVA **NL 855864771B01**. Si ricorda che l'estrazione delle informazioni deve essere imputata al settimo giorno solare antecedente alla data corrispondente alla chiusura della presente RFI. Tale data è importante esplicitarla nella reportistica;
- L'Operatore Economico è tenuto a dichiarare la/le banca/banche dati interrogata/e ai fini della rappresentazione degli Use Case descritti nel presente documento;
- In relazione allo Use Case n°6, l'Operatore Economico può valorizzare le reportistiche anche con dati fittizi in modo da rappresentare le funzionalità garantite dalla piattaforma.

01 Data Entry

Progetto Digital Due Diligence – Data Entry (1 di 2)

La piattaforma deve garantire l'**inserimento** dei dati concernenti l'operazione e i soggetti sottoposti a verifiche reputazionali.

Per quanto riguarda i dati concernenti l'operazione:

- **Tipologia operazione**, es.: Operazione straordinaria; adesione ad associazione; sponsorizzazione; partnership; co-marketing; consulenza; ALTRO (selezionabile da parte dell'utilizzatore tramite menù a tendina più campo "altro" per inserimento testo libero);
- **Area geografica/Paese:** selezionabile da parte dell'utilizzatore tramite menù a tendina più campo "altro" per inserimento testo libero;
- **Nominativo e ruolo controparti**, es. acquirenti, venditori, partner di joint venture, ecc.
- Eventuali altre informazioni su campo libero.

Progetto Digital Due Diligence – Data Entry (2 di 2)

Per quanto riguarda i dati concernenti i soggetti sottoposti a verifiche reputazionali (laddove applicabili, a seconda che si tratti di persone fisiche, persone giuridiche o altre entità):

- Nome / Ragione o denominazione sociale
- Data e luogo di costituzione / Data e luogo di nascita
- Data e numero di iscrizione registro delle società
- Sede Legale / Residenza
- Sede Principale, degli affari (se Diversa dalla Sede Legale) / Domicilio (se diverso dalla residenza)
- Partita IVA / Codice Fiscale
- Area/e di attività
- Forma legale
- Numero di dipendenti
- Ricavi annui ultimi 3 esercizi

Nella maschera di data entry, la piattaforma deve garantire l'inserimento dei dati di tale sezione.

02 Somministrazione Questionario

Progetto DDD – Somministrazione Questionario in Pre-Due Diligence

Preliminarmente alla valutazione reputazionale attraverso l'interrogazione della banca dati, possono essere necessarie e/o opportune (ad es. in base alla normativa aziendale del Gruppo o in base alla valutazione nel caso oggetto di analisi) **attività propedeutiche** come la **Somministrazione di uno o più questionari** alle terze parti.

In particolare, la piattaforma deve consentire la compilazione online a cura della terza parte di uno o più questionari somministrati, che possono presentare alert in caso di mancato completamento di alcuni campi richiesti, nonché il caricamento di eventuale documentazione a corredo (es. Bilanci, Statuto, Atto Costitutivo, etc.)

03 Ricostruzione dell’assetto proprietario

Progetto DDD – Ricostruzione assetto proprietario in Pre-Due Diligence

Preliminarmente alla valutazione reputazionale attraverso l'interrogazione della banca dati, possono essere necessarie e/o opportune (ad es. in base alla normativa aziendale del Gruppo o in base alla valutazione nel caso oggetto di analisi) **attività propedeutiche** quale la **Ricostruzione dell'assetto proprietario/struttura organizzativa** della terza parte.

In particolare, la piattaforma deve consentire la:

- ricostruzione degli assetti proprietari (Shareholders e Beneficial owners)
- ricostruzione della struttura organizzativa (Directors, Managers)

Tale ricostruzione avviene tramite recupero di informazioni da info-provider, da effettuarsi **per il tramite del gestore della piattaforma, mediante connettori** verso la/le banca/banche dati scelta/e per il PoC.

La piattaforma deve consentire la possibilità di visualizzare l'assetto di controllo e deve evidenziare Red Flag nei casi di impossibilità di identificare il Beneficial Owner.

04 Analisi reputazionale

Progetto DDD – Analisi reputazionale

La piattaforma deve garantire lo *screening* della terza parte e di tutti i soggetti individuati in base alle precedenti fasi di *data entry* e *pre-due diligence* (es. directors, shareholders, Ultimate Beneficial Owner, altri soggetti rilevanti immessi dall'utilizzatore della piattaforma), mediante l'**Interrogazione di infoprovider**, che deve avvenire almeno sulle seguenti categorie di rischio:

- Adverse Media
- Corruption
- Sanctions list
- Enforcement
- Politically Exposed Persons (PEPs)
- State Owned Entity (SOE)

Deve essere possibile visualizzare il risultato attraverso la modalità standard prevista dalla piattaforma.

05 Report Due Diligence e Archiviazione

Progetto DDD – Report DD e Archiviazione

La piattaforma deve garantire la creazione di un report di sintesi che abbia come **contenuto minimo sostanziale** le risultanze delle interrogazioni e l'esito delle analisi effettuate (in allegato una proposta di Report utile a comprendere le informazioni necessarie).

La piattaforma deve essere in grado di archiviare i report (e l'eventuale documentazione allegata) secondo la data di ricerca/analisi al fine di garantire la storicizzazione dei dati.

Report

06 Reportistica in materia di Due Diligence

Progetto DDD – Reportistica in materia di Due Diligence

La piattaforma deve dimostrare la capacità di produrre reportistiche, esportabili in diversi formati (Excel, Power Point, PDF e Word) che diano evidenza, a titolo esemplificativo:

a) dell'**elenco** e del **numero di Due Diligence attivate e/o concluse nel periodo di riferimento** (con intervallo temporale impostabile per mese, trimestre, anno, etc.);
b) della **tipologia** di Due Diligence attivate e/o concluse nel periodo di riferimento (i.e. Sponsorizzazioni, Associazioni, Promotori e Consulenti Commerciali, Business Partner, Fornitori, etc.);
c) dell'**esito** delle Due Diligence concluse nel periodo di riferimento (es. % di DD concluse con "esito positivo", % di DD concluse con "esito con criticità non significative e/o mitigabili", % di DD concluse con "esito critico");
d) delle **statistiche** con riferimento alle **Red Flags maggiormente rilevate** (es. % di DD per le quali è presente la red flags "Titolare Effettivo non identificabile", o "catena societaria complessa" o "Presenza in liste PEP", etc.).

Allegato 2

GRUPPO FERROVIE DELLO STATO ITALIANE

REQUEST FOR INFORMATION

Specifiche Tecniche

Piattaforma per la Due Diligence

INDICE

1 SCOPO DELLA REQUEST FOR INFORMATION

Il Gruppo FS, leader nel trasporto passeggeri e merci, gioca un ruolo chiave nel rilancio e sviluppo del sistema della mobilità del Paese e nel sostenere la diversa domanda di mobilità passeggeri, lo spostamento multimodale, l'efficientamento della catena logistica, e integrazione tra diverse infrastrutture all'insegna della sostenibilità.
Il Gruppo FS punta a identificare innovazione, digitalizzazione e connettività come fattori abilitanti del Piano Industriale 2022-2031 attraverso una profonda revisione delle attuali soluzioni tecnologiche.
Per raggiungere questo obiettivo è stato dato un forte impulso alla trasformazione digitale anche attraverso l'introduzione di piattaforme digitali chiave con una forte attenzione alla cultura del dato, alla interoperabilità e resilienza dei sistemi.

A tale proposito, il Gruppo ha lanciato un programma di trasformazione tecnologica che prevede la revisione degli attuali *framework* architetturali Digitali verso uno scenario di *multicloud* ibrido basato su *Common Platforms*, caratterizzato dalla coesistenza di applicazioni *on premise* e *cloud* secondo *best practices* di settore opportunamente applicate al contesto specifico di utilizzo.

OGGETTO DELLA REQUEST FOR INFORMATION

La presente consultazione di mercato viene emessa come strumento di indagine tecnica e di raccolta di informazioni a tutti i fornitori in grado di proporre una soluzione *software* per la:

Piattaforma per la Due Diligence

che risulti pienamente rispondente alle *capabilities* richieste nei paragrafi che seguono, al fine di soddisfare le esigenze del gruppo FS.

2 PIATTAFORMA DI DUE DILIGENCE

La piattaforma avrà una **funzione** di **supporto** alla **Struttura Compliance** di Ferrovie dello Stato Italiane spa nella **gestione** dei processi di ***Due Diligence*** su **Terze parti**. In particolare, la soluzione dovrà supportare il coinvolgimento delle Terze Parti, la valutazione di fattori di rischio, l'interrogazione di specifici *info-provider* e fonti aperte, la ricostruzione dell'assetto proprietario della controparte, la gestione di questionari e documentazione a supporto delle attività.

Nel prossimo paragrafo sono riportati nel dettaglio i requisiti, sulla base dei quali avverrà la valutazione dell'Operatore Economico:

- *Critical Capabilities di tipo funzionale*: elenco delle funzionalità richieste dal Business per lo svolgimento delle attività, quali ad esempio la gestione dei Questionari che innescano la Due Diligence;
- *Critical Capabilities di tipo tecnico*: elenco delle caratteristiche tecniche della piattaforma. Tra queste, la piattaforma deve essere deliverata in modalità SaaS e deve garantire flessibilità e personalizzazione, aggiornamento continuo;
- *Critical Capabilities relative al supporto ed alla manutenzione*: sono stati specificati i requisiti e gli standard da rispettare per l'assistenza e il supporto da parte dell'Operatore Economico (e.g. canali di supporto, lingua di supporto);
- *Requisiti di Sicurezza e Cyber:* sono state specificate le misure di sicurezza da rispettare nell'erogazione del servizio in modalità SaaS.

I requisiti descritti nel documento sono vincolanti ad esclusione di quei requisiti che presentano una nota che li identifica come migliorativi. Agli Operatori Economici si richiede la valutazione di copertura dei requisiti vincolanti e dei requisiti migliorativi compresi all'interno della RFI.

Inoltre, si richiede agli Operatori Economici di predisporre un Proof of Concept (PoC) che permetta di dimostrare che la piattaforma proposta copre effettivamente quanto descritto negli Use Case descritti nel documento "Definizione PoC". Nella fattispecie, all'Operatore Economico che intenda partecipare all'RFI, verrà chiesto di caricare nel Portale Acquisti di Ferservizi SpA sei video o audiovideo dimostrativi della piattaforma, uno per ciascun Use Case. All'Operatore Economico è lasciata la definizione della migliore configurazione delle DEMO della piattaforma con l'obiettivo di rendere i video utili per la valutazione degli Use Case descritti nel documento "Definizione PoC".

Per garantire un equo trattamento di tutti i partecipanti, a ciascun Operatore Economico è richiesta la predisposizione dei video che attestino il completamento delle attività oggetto di PoC, entro le tempistiche definite. Per maggiori dettagli si farà riferimento a comunicazioni successive.

2.1 CRITICAL CAPABILITIES DI PIATTAFORMA

ID	Critical Capabilities di tipo funzionale	
RF1	Data Entry	La piattaforma deve garantire l'inserimento dei seguenti dati concernenti l'operazione: - Tipologia operazione: Operazione straordinaria; adesione ad associazione; sponsorizzazione; partnership; co-marketing; consulenza; Altro (selezionabile da parte dell'utilizzatore tramite menù a tendina più campo "altro" per inserimento testo libero); - Area geografica/Paese: Il campo Area geografica/Paese potrà essere precompilato in automatico dalla piattaforma sulla base della localizzazione geografica dei soggetti sottoposti a verifiche; - Nominativo e ruolo controparti: I nominativi, oltre a essere aggiunti manualmente dall'utilizzatore, potranno essere precompilati in automatico dalla piattaforma sulla base di altri dati inseriti sui soggetti sottoposti a verifiche (es. partita IVA; analogo identificativo estero; identificativo in specifica banca dati); - Eventuali altre informazioni su campo libero.
RF2	Data Entry	La piattaforma deve garantire l'inserimento dei seguenti dati concernenti i soggetti sottoposti a verifiche reputazionali (laddove applicabili, a seconda che si tratti di persone fisiche, persone giuridiche o altre entità: - Nome / Ragione o denominazione sociale - Data e luogo di costituzione / Data e luogo di nascita - Data e numero di iscrizione registro delle società - Sede Legale / Residenza - Sede Principale, degli affari (se Diversa dalla Sede Legale) / Domicilio (se diverso dalla residenza) - Partita IVA / Codice Fiscale - Area/e di attività - Forma legale - Numero di dipendenti - Ricavi annui ultimi 3 esercizi I dati di tale sezione dovranno essere, nella massima misura possibile, precompilati in automatico dalla piattaforma sulla base di altri dati inseriti sui soggetti sottoposti a verifiche (es. partita IVA; analogo identificativo estero; identificativo in specifica banca dati), ferma restando la possibilità di essere modificati/integrati manualmente dall'utilizzatore anche attraverso campi a testo libero.
RF3	Schede	La piattaforma deve consentire la compilazione di moduli online, sia da parte di personale di altre società/strutture del Gruppo abilitate sia da parte di soggetti terzi
RF4	Tracciatura Informazioni	Le operazioni a sistema devono essere tracciate, riconoscendo l'utente che le ha effettuate
RF5	Notifiche	La piattaforma deve permettere l'invio di notifiche agli attori interessati al momento del caricamento dei documenti

ID	Critical Capabilities di tipo funzionale	
RF6	Note	La piattaforma deve permettere l'inserimento di note a corredo di ciascun documento caricato a sistema
RF7	Data Retention	La piattaforma deve consentire una diversificazione dell'impostazione di data retention a seconda della tipologia della controparte
RF8	Attivazione Due Diligence	La piattaforma deve permettere l'attivazione della Due Diligence tramite compilazione a sistema da parte della Struttura Richiedente di un form preliminare.
RF9	Form preliminare	Il form preliminare, che innesca l'attività di Due Diligence, deve poter essere customizzabile
RF10	Pre-Scoring	Preliminarmente alla valutazione reputazionale, la piattaforma deve permettere l'attività di prescoring che consente un calcolo automatico sulla base di indicatori predeterminati, che possano essere configurati e/o suggeriti dalla piattaforma, quali ad esempio: - Livello di rischio del Paese di sede/residenza della terza parte e/o del Paese di riferimento dell'operazione; - Rischio del settore di attività della terza parte e/o settore di riferimento dell'operazione; - Elementi di complessità nella compagine della terza parte; - Presenza di altre red flags
RF11	Analisi rischio	La piattaforma deve, in base alle risposte fornite nel form preliminare (Questionario Interno) assegnare un livello di rischio iniziale alla controparte (Alto, Medio, Basso), con possibilità di riclassificazione dell'esito della valutazione, corredata da un campo note
RF12	Controlli differenziati	La piattaforma deve garantire l'implementazione di controlli differenziati in funzione del livello di rischio iniziale assegnato alla controparte
RF13	Questionari esterni	La piattaforma deve permettere la somministrazione di questionari (questionari esterni) a terze parti
RF14	Questionari esterni	La piattaforma deve consentire di inserire nei questionari sia domande a risposta chiusa che aperta.
RF15	Questionari esterni	A seguito della compilazione del Questionario da una Terza Parte, la piattaforma garantisce una modalità che permette di certificare l'autenticità del compilatore.[1]
RF16	Questionari esterni	La piattaforma deve consentire di inserire nei questionari il controllo automatico di mancata compilazione dei campi, prevedendo campi obbligatori con alert in caso di mancato completamento.
RF17	Accesso Terze parti	La piattaforma deve garantire l'accesso alle terze parti attraverso specifici meccanismi (es. con meccanismi di One Time Password).

[1] Il requisito è da considerarsi migliorativo.

ID	Critical Capabilities di tipo funzionale	
RF18	Allegati	La piattaforma deve garantire alla terza parte la possibilità di allegare la documentazione a corredo (es. Bilanci, Statuto, Atto Costitutivo, etc.)
RF19	Canali comunicazione	La piattaforma deve garantire alla terza parte la possibilità di utilizzare l'area di chat per comunicare con la struttura richiedente
RF20	Analisi rischio	L'analisi del rischio, effettuata automaticamente dalla piattaforma, deve tener conto di controlli standard
RF21	Analisi rischio	L'analisi del rischio, effettuata automaticamente dalla piattaforma, deve tener conto di controlli aggiuntivi nel caso in cui il livello di rischio sia incrementato
RF22	Analisi rischio	L'analisi del rischio, effettuata automaticamente dalla piattaforma, deve tener conto di rivalutazioni manuali del rischio
RF23	Analisi rischio	L'analisi del rischio, effettuata automaticamente dalla piattaforma, deve verificare la presenza di eventuali Red Flag
RF24	Analisi rischio	L'analisi del rischio, effettuata automaticamente dalla piattaforma, deve tener conto della definizione di un piano di mitigazione degli eventuali Red Flag
RF25	Analisi rischio	La piattaforma, a valle dell'analisi del rischio, deve calcolare il rischio finale
RF26	Analisi rischio	L'analisi del rischio, effettuata automaticamente dalla piattaforma, deve tener conto del profilo approvativo in base ai Red Flag e al piano di mitigazione
RF27	Analisi sulla controparte	La piattaforma deve permettere l'analisi della controparte considerando la Ricostruzione degli assetti proprietari tramite recupero di informazioni da info-provider attraverso connettori
RF28	Analisi sulla controparte	La piattaforma, nell'analisi della controparte, deve garantire il settaggio del valore soglia relativo alla percentuale di partecipazione proprietaria oltre la quale estendere i controlli sui soggetti
RF29	Analisi sulla controparte	La piattaforma deve permettere la ricostruzione della struttura organizzativa tramite recupero di informazioni da info-provider attraverso connettori alle banche dati
RF30	Analisi sulla controparte	La piattaforma deve garantire lo screening della terza parte e di tutti i soggetti individuati in base alle precedenti fasi di data entry e pre-due diligence (es. directors, shareholders, Ultimate Beneficial Owner, altri soggetti rilevanti immessi dall'utilizzatore della piattaforma), mediante l'interrogazione di infoprovider specializzati attualmente in uso (Bureau van Dijk, RDC On Board e Refinitiv World Check One, ferma restando la possibilità di integrare l'elenco degli infoprovider con ulteriori database di informazioni commerciali), che deve avvenire almeno sulle seguenti categorie di rischio: Adverse Media, Corruption, Sanctions list, Enforcement, Politically Exposed Persons (PEPs), State Owned Entity (SOE)
RF31	Analisi sulla controparte	La piattaforma deve avere un connettore nativo con l'info-provider Dun & Bradstreet (controparti estere)

ID	Critical Capabilities di tipo funzionale	
RF32	Analisi sulla controparte	La piattaforma deve avere un connettore nativo con l'info-provider Bureau van Dijk (controparti italiane ed estere)
RF33	Analisi sulla controparte	La piattaforma deve avere un connettore nativo con l'info-provider RDC on Board
RF34	Analisi sulla controparte	La piattaforma deve avere un connettore nativo con l'info-provider Refinitiv World Check One
RF35	Analisi sulla controparte	La piattaforma deve avere un connettore nativo con l'info-provider Cribis (controparti italiane)
RF36	Visualizzazione Assetto	La piattaforma deve consentire la possibilità di visualizzazione grafica dell'assetto di controllo
RF37	Visualizzazione Assetto	La piattaforma deve consentire la possibilità di visualizzare in forma tabellare l'assetto di controllo
RF38	Red Flag	La piattaforma deve consentire la possibilità di evidenziare Red Flag nei casi di impossibilità di identificare il Beneficial Owner.
RF39	Analisi reputazionale multi-sorgente	La piattaforma deve garantire l'esecuzione di verifiche su strutture proprietarie di controllo, nonché Directors e Managers importando le informazioni derivate dall'info-provider. Tali dati dovranno essere, nella massima misura possibile, precompilati in automatico dalla piattaforma sulla base di altri dati inseriti sui soggetti sottoposti a verifiche (es. partita IVA; analogo identificativo estero; identificativo in specifica banca dati).
RF40	Analisi reputazionale multi-sorgente	La piattaforma deve garantire la possibilità di inserire/modificare manualmente nominativi di soggetti per i quali è necessaria la verifica reputazionale, anche attraverso campi a testo libero
RF41	Analisi reputazionale multi-sorgente	La piattaforma deve consentire l'esecuzione di ricerche sul web per trovare Adverse Media sulle singole entità identificate durante l'esecuzione dei controlli precedenti, dando evidenza di potenziali Red Flag e/o di eventuali falsi positivi
RF42	Analisi reputazionale multi-sorgente	La piattaforma deve consentire l'esecuzione di ricerche sul web in lingua italiana
RF43	Analisi reputazionale multi-sorgente	La piattaforma deve consentire l'esecuzione di ricerche sul web in lingua inglese
RF44	Analisi reputazionale multi-sorgente	La piattaforma consente l'esecuzione di ricerche sul web in lingua francese[2]

[2] Il requisito è da considerarsi migliorativo.

ID	Critical Capabilities di tipo funzionale	
RF45	Analisi reputazionale multi-sorgente	La piattaforma consente l'esecuzione di ricerche sul web in lingua spagnola[3]
RF46	Report di Due Diligence	La piattaforma deve garantire la produzione e validazione del Report di Due Diligence
RF47	Report di Due Diligence	Il Report prodotto dalla piattaforma deve riportare la valutazione finale del livello di rischio associato alla controparte
RF48	Report di Due Diligence	Il Report prodotto dalla piattaforma deve riportare le evidenze dei Red Flags emersi nelle fasi precedenti
RF49	Report di Due Diligence	Il Report prodotto dalla piattaforma deve permettere l'eventuale inserimento di proposte da parte di Compliance (da inserire in un campo note a testo libero) a mitigazione delle Red Flags identificate.
RF50	Report di Due Diligence	La piattaforma deve essere in grado di archiviare i report (e l'eventuale documentazione allegata) secondo la data di ricerca/analisi al fine di garantire la storicizzazione dei dati.
RF51	Validazione analisi reputazionale	Nella fase di validazione dell'analisi reputazione, la piattaforma deve consentire la modifica dei risultati delle interrogazioni, eliminando i risultati ritenuti c.d. "falsi positivi", anche secondo criteri di scrematura automatica dei falsi positivi, a condizione che delle corrispondenze scartate venga mantenuta evidenza e possano essere ripristinate a giudizio dell'utilizzatore della piattaforma.
RF52	Validazione analisi reputazionale	Nella fase di validazione dell'analisi reputazionale, la piattaforma deve consentire la modifica dei risultati delle interrogazioni, mitigando o innalzando manualmente livelli/elementi di rischio rilevati automaticamente dalla piattaforma stessa.
RF53	Validazione analisi reputazionale	Nella fase di validazione dell'analisi reputazione, la piattaforma deve consentire la modifica dei risultati delle interrogazioni, aggiungendo note a testo libero e allegando documenti.
RF54	Processo di Due Diligence	La piattaforma deve consentire, in tutte le fasi di processo, di inserire note e valutazioni delle risultanze della Due Diligence delle valutazioni dei Red Flags, nonché di allegare ulteriore documentazione (es. tratta da fonti esterne o Report di Due Diligence prodotti da fornitori specializzati)
RF55	Processo di Due Diligence	La piattaforma deve gestire diversi livelli approvativi (tramite Workflow)
RF56	Organigrammi	La piattaforma deve poter gestire gli organigrammi e le variazioni agli stessi
RF57	Notifiche	La piattaforma deve inviare notifiche sulle attività pending

[3] Il requisito è da considerarsi migliorativo.

ID	Critical Capabilities di tipo funzionale	
RF58	Dashboard	Ciascun utente, nel momento in cui si collega al sistema, deve poter visualizzare una maschera riepilogativa delle attività a suo carico
RF59	Report	La piattaforma deve predisporre Report sia in fase di avanzamento delle Due Diligence (stato di avanzamento, profilo di rischio, Red Flags emerse, workflow approvativi differenziati in caso di escalation) sia in fase di output (le informazioni raccolte nel processo di analisi, risk scoring, informazioni preliminari, evidenze di Red Flags, ecc.)
RF60	Ricerca	La piattaforma deve consentire la ricerca full text nelle sezioni
RF61	Ricerca	La piattaforma deve consentire la ricerca full text nei documenti allegati
RF62	Export informazioni	La piattaforma deve consentire l'export delle informazioni presenti in piattaforma sui principali formati file della Suite Office)
RF63	Export informazioni	La piattaforma deve consentire l'export delle informazioni presenti in piattaforma in formato PDF
RF64	Reporting	La piattaforma deve predisporre reporting tramite cruscotti dedicati
RF65	Alert	La piattaforma permette la ricezione di eventuali alert trasmessi tramite le funzionalità di monitoraggio continuo disponibili sulle banche dati, fornita da Infoprovider esterni tramite API.[4]
RF66	Due Diligence precedenti	La piattaforma permette di attualizzare le Due Diligence svolte in passato[5]
RF67	Collegamento a Due Diligence precedenti	La piattaforma consente di creare collegamenti/link con Report di Due Diligence già concluse[6]

ID	Critical Capabilities di tipo tecnico	
RT1	SaaS Platform	La piattaforma deve essere deliverata in modalità SaaS (Software as a Service).
RT2	Web-based app	La piattaforma deve essere web based ovvero accessibile da web.
RT3	Responsive	La Piattaforma deve essere responsive, in modo che si possa visualizzare e usufruire da ogni browser, device (cellulare, computer, tablet, etc.) e sistema operativo e browser. In particolare, da Mobile per Android a partire dalla versione 6.0 in poi - IOS da versione IOS 10 in poi.

[4] Il requisito è da considerarsi migliorativo.
[5] Il requisito è da considerarsi migliorativo.
[6] Il requisito è da considerarsi migliorativo.

ID	Critical Capabilities di tipo tecnico	
RT4	Accesso alla piattaforma per i dipendenti del Gruppo FS	I dipendenti del Gruppo FS devono essere autenticati e autorizzati sulla piattaforma con supporto del protocollo Azure Active Directory
RT5	Profilazione	La piattaforma deve permettere di definire dei ruoli e di profilare gli utenti in modo da gestire i coni di visibilità ed i permessi sulla base di specifici parametri ed esigenze (es. società, struttura organizzativa, ecc.).
RT6	Scalabilità	La piattaforma deve essere scalabile e permettere di aggiungere maggiori risorse con l'obiettivo di supportare un numero crescente di utenti, società, documenti e dati in generale rispetto alla baseline.
RT7	Compatibilità a fronte di nuove realease della piattaforma	L'Operatore Economico deve assicurare, a fronte di rilasci di nuove versioni principali o secondarie della piattaforma (major/minor release), la compatibilità con tutte le configurazioni/personalizzazioni effettuate per rispondere all'esigenze dell'organizzazione, nonché la compatibilità con le integrazioni attivate con i sistemi del Gruppo FS. Inoltre, l'Operatore Economico deve descrivere, mediante documentazione opportuna, il processo e le modalità di aggiornamento dell'applicazione SaaS, indicando in maniera trasparente e chiara l'impatto di ogni operazione sulle funzionalità del servizio. L'Operatore Economico deve condividere il piano e le modalità di test end to end delle modifiche apportate.
RT8	Integrazione via Web Services	La piattaforma deve consentire l'integrazione con altri servizi tramite Web Services e API.
RT9	Integrazione con altri sistemi aziendali	La piattaforma deve consentire l'integrazione con la suite Microsoft Office365.
RT10	Integrazione con altri sistemi aziendali	La piattaforma deve consentire l'integrazione Sharepoint.
RT11	Integrazione con altri sistemi aziendali	La piattaforma deve consentire l'integrazione con altri sistemi aziendali: es. SAP BW/4, SAP S/4, SAP Ecc, SAP BW Netweaver, SAP HR.
RT12	Integrazione con altri sistemi aziendali	Il sistema deve consentire l'integrazione con la piattaforma Oracle Enterprise Performance Management.
RT13	Estrazione completa dei dati	Deve essere sempre possibile, da parte di FS Technology, l'estrazione di una copia completa dei dati memorizzati e gestiti dal servizio (in formato standard, non proprietario e riutilizzabile), ivi compresi i dati derivati quali log e statistiche di utilizzo, nonché le configurazioni del servizio.

ID	Critical Capabilities di tipo tecnico	
RT14	Migrazione verso altra applicazione	Al termine del contratto, deve essere prevista un'attività di migrazione dei dati del servizio verso un'altra applicazione con conseguente eliminazione permanente dei dati di proprietà del Gruppo FS al termine della procedura di migrazione (inclusi i dati derivati e i dati di backup). Per quanto riguarda i documenti, i file dovranno essere esportati in formato originale, o in altro formato standard di mercato, secondo quanto indicato dal Committente. Dovrà essere fornita dettagliata ed esaustiva documentazione delle modalità di indicizzazione e di archiviazione dei documenti (metadati, IdC, etc.) per consentire un'agevole presa in carico dei documenti restituiti.
RT15	Ambienti	Il servizio deve consentire la separazione degli ambienti in sviluppo, certificazione e produzione, con il rispetto dei passaggi previsti per favorire l'esecuzione delle attività di sviluppo e testing in modo controllato e sicuro (non prevedendo l'utilizzo di dati reali in ambienti di test e sviluppo).
RT16	Utenze di test	L'Operatore Economico SaaS deve rendere disponibile un account di test per ogni ruolo ed un URL utilizzabili dall'acquirente per effettuare ogni tipo di verifica necessaria per il rilascio di nuove evolutive.
RT17	Change Management	Adozione di procedure/strumenti di change management per tenere traccia delle modifiche eseguite sulle configurazioni del sistema.
RT18	Personalizzazione /configurazione interfaccia	Il sistema gode di flessibilità sufficiente per l'adattamento dei form e la configurazione dell'interfaccia rispetto alle specifiche funzionali e di layout previste in fase di progettazione.
RT19	Creazione reportistica	Il sistema dovrà essere in grado di produrre Report predefiniti standard e custom in formato Word, Pdf, Power Point ed Excel.
RT20	Integrazione con altri sistemi aziendali	La piattaforma consente l'integrazione con la piattaforma Salesforce[7]

ID	Critical Capabilities relative al supporto ed alla manutenzione	
S1	Presenza in Italia	L'Operatore Economico deve avere sedi in Italia in grado di erogare supporto.
S2	Supporto tecnico e supporto operativo agli Utenti FSTechnology gestori	È richiesto all'Operatore Economico di erogare supporto tecnico e supporto operativo agli utenti FSTechnology gestori della piattaforma per tutta la durata del contratto.
S3	Supporto tecnico e supporto operativo agli Utenti finali	È richiesto all'Operatore Economico di erogare supporto tecnico e supporto operativo agli utenti finali per l'utilizzo della piattaforma per tutta la durata del contratto.

[7] Il requisito è da considerarsi migliorativo.

ID	Critical Capabilities relative al supporto ed alla manutenzione	
S4	Canali di supporto base	L'Operatore Economico deve garantire il supporto al Gruppo FS attraverso i seguenti canali: e-mail.
S5	Canali di supporto base	L'Operatore Economico deve garantire il supporto al Gruppo FS attraverso un canale ticketing.
S6	Canali di supporto extra	L'Operatore Economico garantisce il supporto al Gruppo FS attraverso un canale telefonico.[8]
S7	Canali di supporto extra	L'Operatore Economico garantisce il supporto al Gruppo FS attraverso un canale live chat[9]
S8	Sistema di trouble ticketing	L'Operatore Economico deve allestire un sistema di trouble ticketing di tipo web-based, per la raccolta e la piena condivisione a FSTechnology delle difformità e dei disservizi riscontrati durante l'esercizio. In particolare, il sistema deve consentire: - il monitoraggio in maniera autonoma dei ticket aperti e del loro stato di elaborazione; - la generazione di reportistica relativa all'insieme di ticket aperti in un determinato periodo di riferimento.
S9	Integrazione canale di supporto ticketing	L'Operatore Economico supporta FSTechnology attraverso un canale ticketing integrabile con i sistemi di governance IT. Per garantire l'interoperabilità, occorre disporre di un web service di tipo SOAP o REST[10]
S10	Orari supporto minimo	Il supporto deve essere garantito: - 5 giorni alla settimana lavorativi secondo il calendario italiano; - orario 8-18 nei giorni lavorativi del calendario italiano.
S11	Orari supporto	Il supporto è garantito: - 7/7 giorni alla settimana secondo il calendario italiano; - 24 ore su 24 nei giorni lavorativi del calendario italiano. [11]
S12	Lingua supporto	Il supporto dell'Operatore Economico deve essere in Lingua Italiana.
S13	Lingua supporto	Il supporto dell'Operatore Economico è disponibile anche in Lingua Inglese. [12]
S14	Recovery Time Objective (RTO)	Recovery Time Objective (RTO, inteso come il massimo tempo di indisponibilità del servizio) pari a 4 ore. Formula per il calcolo NRTO = numero di eventi di fermo con mancato rispetto del RTO Periodo di riferimento per il calcolo: mensile.
S15	Disponibilità del servizio	Disponibilità del servizio su base mensile pari ad almeno il 98% delle ore totali (nel calcolo della disponibilità del servizio non saranno considerate interruzioni

[8] Il requisito è da considerarsi migliorativo.
[9] Il requisito è da considerarsi migliorativo.
[10] Il requisito è da considerarsi migliorativo.
[11] Il requisito è da considerarsi migliorativo.
[12] Il requisito è da considerarsi migliorativo.

ID	Critical Capabilities relative al supporto ed alla manutenzione	
		dovute a eventi di forza maggiore, inteso come un evento al di fuori del controllo dell'Operatore Economico o dovute a interventi manutentivi).
S16	Tempo di presa in carico	Tempo di presa in carico pari a 4 ore negli orari del supporto dalla segnalazione/richiesta di intervento.
S17	Tempo di risoluzione del malfunzionamento in caso di errori bloccanti	Tempo di risoluzione del malfunzionamento in caso di errori bloccanti pari a 12 ore dalla presa in carico.
S18	Risoluzione malfunzionamenti non bloccanti	Tempo di risoluzione del malfunzionamento non bloccante entro massimo 36 ore dalla presa in carico.

ID	Requisiti di Sicurezza e Cyber	
C.O.1	Ruoli e Responsabilità definiti formalmente in ambito Data Protection	Identificazione dei ruoli e delle responsabilità associate alle persone coinvolte nel trattamento dei dati
C.O.2	Formazione periodica in ambito Data Protection	Esistenza di corsi in aula o E-learning, newsletter, pillole formative periodiche per accrescere la conoscenza delle tematiche relative alla Data Protection
C.O.3/9	Svolgimento audit di sicurezza periodici e verifica in materia Data Protection	Esistenza di un processo periodico relativo all'esecuzione di audit di sicurezza, inclusa la verifica della conformità normativa in ambito Data Protection
C.O.4	Monitoraggio periodico delle non conformità normative in ambito Data Protection	Esistenza di un processo periodico di monitoraggio delle non conformità normative rilevate nei precedenti audit
C.O.5	Policy di sicurezza	Esistenza di politiche di sicurezza delle informazioni dell'intera organizzazione
C.O.6	Modello di controlli IT	Definizione di un set di controlli IT da implementare basati sui principali standard

ID	Requisiti di Sicurezza e Cyber	
C.O.7	Certificazione del sistema di sicurezza	Verifica di un sistema per l'acquisizione di un certificato che attesti che quel dato sistema soddisfa i requisiti di sicurezza dettati dall'entità certificatrice
C.O.8	Risk Assessment periodici	Devono essere periodicamente (almeno annualmente) effettuate delle sessioni di analisi, valutazione e trattamento dei rischi.
C.O.9	Implementazione inventario HW/SW	Implementare un inventario dei dispositivi hardware e del software di proprietà dell'organizzazione.
C.O.10	Policy per la gestione degli accessi ai sistemi informatici	Esistenza di politiche per la gestione degli accessi ai sistemi informatici
C.O.11	Review periodica delle utenze	Esistenza di un processo di revisione periodica delle utenze profilate nei sistemi
C.O.12	Policy per la gestione del ciclo di vita del software (Secure SDLC)	Esistenza di una politica che definisce un ciclo di sviluppo sicuro del software secondo gli attuali standard di settore (es. OWASP)
C.O.13	Formazione sullo sviluppo sicuro	Assicurare che il personale che sviluppa abbia ricevuto un'adeguata formazione sulla scrittura di codice sicuro nel loro specifico ambiente di sviluppo.
C.O.14	Policy per la gestione degli incidenti di sicurezza	Esistenza di politiche di gestione degli incidenti di sicurezza.
C.O.15	Istruzioni operative per l'utilizzo delle risorse informatiche e internet	Definizione e implementazione di istruzioni operative per l'utilizzo delle risorse informatiche e internet
C.O.16	Istruzioni operative per la cancellazione sicura dei dispositivi	Esistenza di una procedura che preveda la possibilità di cancellare in modo sicuro i dati dai dispositivi che trattano dati personali

ID	Requisiti di Sicurezza e Cyber	
C.O.17 /18	Clausola contrattuali, SLA e processo di monitoraggio dell'operato delle Terze Parti o "persone correlate"	Definizione degli indicatori di prestazione chiave tra il Responsabile e le "persone correlate" ad esso, al fine di fornire il livello di servizio desiderato e di revisionare periodicamente l'operato delle persone correlate.
C.O.18	Reputation e Data Breach	E' necessario definire ed implementare un processo per tutelare la presenza sul web dell'organizzazione. In particolar modo identificare siti illegittimi e monitorare il web per identificare potenziali data breach.
C.O.19	Misure prescrittive per amministratori di sistema	Esistenza di specifiche misure di sicurezza che devono essere adottate dagli amministratori di sistema
C.O.21	Backup - Definizione policy	Deve essere definita ed implementata una opportuna policy per la gestione del backup.
C.O.22	Public Key Infrastructure - Processo di gestione chiavi di cifratura	Deve essere definito e documentato un processo per la gestione del ciclo di vita delle chiavi di cifratura / mascheramento dati (creazione, archiviazione, recupero, distribuzione, ritiro e distruzione).
C.O.23	Public Key Infrastructure - Nomina dei responsabili delle chiavi di cifratura	Devono essere nominati i responsabili delle chiavi di cifratura / mascheramento dati e sensibilizzati sulle proprie responsabilità nell'uso e protezione delle chiavi.
C.O.24	Ruoli e responsabilità in ambiente cloud	Devono essere definiti, registrati e comunicati in modo chiaro i ruoli e le responsabilità (in condivisione o suddivisione) in carico all'organizzazione e al Cloud Provider.
C.O.26	Localizzazione dei Data Center	I datacenter e le informazioni/servizi in Cloud devono risiedere su territorio nazionale o all’interno dell’Unione Europea
C.O.27	Notifica data breach da parte del Cloud Provider	Il Cloud Provider deve segnalare tempestivamente all'organizzazione eventuali accessi non autorizzati a dati soggetti a regolamento GDPR, che possano causare perdite, divulgazioni o alterazioni dei dati.
C.O.28	Accordi di non divulgazione (Non Disclosure Agreement, NDA)	Il personale del Cloud Provider avente accesso a dati riservati deve essere soggetto ad obblighi di riservatezza

ID	Requisiti di Sicurezza e Cyber	
C.O.31	Processo formale di Change & Patch management	Definizione di un processo formale che documenti la fase di autorizzazione e implementazione delle modifiche e dell'installazione delle patch all'interno di processi, sistemi o strutture aziendali
C.T.1	Meccanismi di identificazione e autenticazione	Esistenza di meccanismi di accesso ai sistemi tramite il riconoscimento attraverso un nome utente e l'autenticazione attraverso password.
C.T.2	Utilizzo utenze univoche e nominali	Esistenza di utenze che siano associate in modo univoco a persone fisiche, identificabili con nome e cognome e/o riconducibili univocamente ad un unico soggetto responsabile
C.T.3	Meccanismi di autorizzazione	Implementazione di controlli che permettano di definire quali operazioni possa compiere uno specifico utente
C.T.4	Gestione utenze Privilegiate	Implementazione di controlli specifici sulle utenze con privilegi ampi per impedire operazioni illecite
C.T.5	Password policy conforme alle linee guida aziendali	Insieme di regole che definiscono come dovrebbe essere costituita una password affinché possa essere ritenuta sufficientemente sicura; tale misura è associata alle utenze interne (non clienti).
C.T.6	Strong Authentication	Esistenza di un sistema di autenticazione forte o a 2 fattori (es. password + one time password)
C.T.7	Accesso logico terze parti	L'accesso logico ai sistemi da parte di terzi (ad esempio clienti, fornitori, consulenti) deve essere soggetto a controlli rigorosi.
C.T.8	Tracciamenti accessi utenti	Registrazione e memorizzazione dei log degli accessi degli utenti (es. login, logout e principali attività utente, ad esempio download di dati, cancellazione di dati, modifiche massive dei dati)
C.T.9	Tracciamento accessi Amministratori di Sistema	Registrazione e memorizzazione dei log degli accessi degli Amministratori di Sistema (es. login, logout e principali attività utente, ad esempio download di dati, cancellazione di dati, modifiche massive dei dati)
C.T.10	Protezione dei log	Esistenza di meccanismi di protezione dei log in maniera da non poter essere cancellati da personale non autorizzato.
C.T.11	Retention dei log	Esistenza di un limite temporale entro il quale possano essere conservati i log
C.T.12	Tracciamento degli Incident	Registrazione e memorizzazione degli incidenti avvenuti/individuati
C.T.13	Network Time Protocol (NTP)	Configurazione del protocollo NTP al fine di sincronizzare il clock del sistema
C.T.14	Monitoraggio delle performance	Attività di monitoraggio delle performance del sistema in modo da verificare che siano rispettati i livelli di servizio stabiliti

ID	Requisiti di Sicurezza e Cyber	
C.T.15	Invio Log a piattaforma di analisi e correlazione eventi (es: SIEM, CASB)	Reindirizzamento dei log dei vari sistemi all'interno di un sistema centralizzato che si occupa della correlazione degli eventi e dell'analisi di eventuali anomalie
C.T.16 /17	Sistema monitorato da SOC h24	Sistema soggetto a monitoraggio real time 24 ore su 24 da parte di un centro altamente specializzato nell'individuazione di eventuali anomalie nei sistemi e nelle reti
C.T.18	Cifratura dei canali di trasmissione (HTTPS)	Esistenza di tecniche e protocolli per la protezione dei dati durante le transazioni (es. https)
C.T.19 /20	Hardening dei sistemi	Implementazione di specifiche configurazioni su sistemi e componenti che permettono di incrementare la sicurezza di un sistema.
C.T.21	Strumenti e Metodologie di Threat Intelligence	Deve essere definito e implementato un processo di Threat Intelligence, per raccogliere, analizzare ed elaborare le informazioni relative alle potenziali minacce che possono impattare l'organizzazione e appositi strumenti e data feed
C.T.22	Host Intrusion Detection System (HIDS)	Utilizzo di Host Intrustion Detection System
C.T.23	Host Intrusion Prevention System (HIPS)	Utilizzo di Host Intrustion Prevention System
C.T.24	Antivirus	Adozione di strumenti di prevenzione e protezione da virus.
C.T.25	Anti-malware	Adozione di strumenti di prevenzione e protezione da malware.
C.T.26	Collezionamento eventi virus su piattaforma centralizzata	Tutti gli eventi virus-related devono essere inviati ad una piattaforma centralizzata di collezionamento.
C.T.27	Collezionamento eventi malware su piattaforma centralizzata	Tutti gli eventi malware-related devono essere inviati ad una piattaforma centralizzata di collezionamento.
C.T.28	Aggiornamento software anti-virus	Il software anti-virus deve essere costantemente aggiornato.
C.T.29	Aggiornamento software anti-malware	Il software anti-malware deve essere costantemente aggiornato.

ID	Requisiti di Sicurezza e Cyber	
C.T.30 /31	Patch Management	Installazione di patch di sicurezza sui sistemi per risolvere le vulnerabilità rilevate
C.T.32	Patch Management tramite tool automatici	Utilizzo di tool automatici per le attività di patch management.
C.T.33	Vulnerability Assessment	Attività periodiche schedulate ed effettuate da sonde in grado di rilevare vulnerabilità sui sistemi operativi ed applicativi.
C.T.34	Penetration Test	Attività di analisi di sicurezza mirate, con lo scopo di rilevare vulnerabilità e simulare attacchi informatici
C.T.35	Simulazione Red Team vs Blue Team	Effettuare periodicamente simulazioni di attacco per testare il livello di efficacia dell'organizzazione nel reagire.
C.T.36	Back up periodico	Effettuazione pianificata di copie di riserva finalizzata a duplicare, con una periodicità prestabilita, i dati, le configurazioni e le immagini di sistema su appositi supporti di memorizzazione.
C.T.37	Disaster recovery	Definizione di procedure per garantire la possibilità di mantenere in piedi un servizio/sistema anche in caso di malfunzionamento, sia di natura accidentale che malevola, e di poter ristabilire in tempi definiti l'operatività completa dei sistemi (è richiesto un piano di Disaster recovery).
C.T.38	Piani di continuità operativa	Definizione di procedure per garantire la possibilità di mantenere in piedi un servizio/sistema anche in caso di malfunzionamento, sia di natura accidentale che malevola, e di poter ristabilire in tempi definiti l'operatività completa dei sistemi (è richiesto un piano di Continuità operativa).
C.T.39	High Availability	Implementazione di un modello che permette, tramite l'adozione di strumenti tecnologici ridondati, di avere un sistema altamente disponibile ai propri utenti.
C.T.40	Test periodici	Implementare periodicamente dei test di ripristino delle copie di backup.
C.T.41	Protezione copie di backup	Le copie di backup devono essere protette mediante opportune misure di sicurezza fisica e logica (protezione da perdite, danni e accessi non autorizzati).
C.T.42	Cifratura copie di backup	Le copie di backup devono essere protette mediante opportune misure di sicurezza fisica e logica (tramite cifratura dati).
C.T.43	Tecniche di cifratura	Esistenza di tecniche di cifratura dei dati memorizzati (es. dati memorizzati nei database o nelle memorie di massa)
C.T.44	Mascheramento dei dati	Esistenza di tecniche di data masking per minimizzare la visualizzazione e lettura di dati personali basati sul principio del "need to know"
C.T.45 /46	Segregazione ambienti	Separazione fisica o virtuale degli ambienti che compongono il sistema (es. sviluppo, test, formazione, produzione)

ID	Requisiti di Sicurezza e Cyber	
C.T.47	Requisiti di sicurezza software fornitori	I fornitori di software devono garantire un adeguato livello di sicurezza del proprio software.
C.T.48	Test su nuovi sistemi	I nuovi sistemi devono essere testati rigorosamente, in accordo con piani di test predefiniti e documentati, e i risultati approvati e firmati, prima dell'installazione in ambiente di esercizio.
C.T.49	Controllo Accessi Fisici	Misure di sicurezza per controllare gli accessi che vengono effettuati al data center che ospita le macchine dell'organizzazione
C.T.50	Antincendio	Misure di sicurezza per prevenire o far fronte ad un possibile incendio del Data Center che ospita le macchine dell'organizzazione
C.T.51	Antiallagamento	Misure di sicurezza per prevenire o far fronte ad un possibile allagamento del Data Center che ospita le macchine dell'organizzazione.
C.T.52	Controllo temperatura data center	Attività di monitoraggio della temperatura interna dei Data Center per tutelare le macchine in esso presenti.
C.T.53	Sicurezza fisica dispositivi di rete	I cavi di rete ed i punti di accesso alla rete devono essere protetti mediante controlli fisici.
C.T.54	Sicurezza fisica degli edifici	Gli edifici che ospitano l'infrastruttura IT dell'organizzazione devono essere fisicamente protetti contro incidenti o attacchi di sicurezza.
C.T.55	Protezione da sbalzi/interruzioni di corrente	Le infrastrutture IT devono essere protette contro sbalzi o interruzioni di corrente.
C.T.56	Input validation	Misure di sicurezza che rafforzano l'applicativo impedendo la possibilità di sfruttare vulnerabilità comuni (e.g. validazione degli input).
C.T.57	Code review	È necessario eseguire dei controlli sul codice applicativo per identificare e indirizzare le vulnerabilità di sicurezza (ad esempio mediante analisi statica e dinamica del codice sorgente e test di unità).
C.T.59	File Integrity Tool	Devono essere utilizzati opportuni strumenti di verifica dell'integrità dei file per assicurare che i file critici di sistema (compresi eseguibili, librerie e file di configurazione) non siano stati alterati.
C.T.60	Protezione Avanzata Database	Le basi di dati contenenti informazioni e dati rilevanti devono essere protette contro l'accesso e la modifica non autorizzati.
C.T.66	Cancellazione base (a livello software)	Utilizzo di algoritmi e meccanismi generici per la cancellazione dei dati

ID	Requisiti di Sicurezza e Cyber	
C.T.67	Decommissioning e cancellazione sicura (a livello hardware)	Attività di dismissione sicura dei dispositivi di archiviazione utilizzati dai sistemi dell'organizzazione.
C.C.1	Web Application Firewall (WAF)	Utilizzo di Web Application Firewall per la protezione dei sistemi
C.C.2	Cifratura dei canali di trasmissione (es: VPN)	Esistenza di tecniche e protocolli per la protezione dei dati durante le transazioni (es. VPN)
C.C.3	Protezione Anti DDOS	Esistenza di sistemi per la protezione da attacchi aventi come obiettivo l'indisponibilità di uno o più servizi
C.C.4	Firewall	Il traffico di rete in ingresso e in uscita dalla rete dell'organizzazione deve essere instradato attraverso un firewall opportunamente configurato e gestito, al fine di bloccare, limitare e monitorare in maniera puntuale, il traffico in transito sulla rete.
C.C.5	Rilevamento intrusioni sulla rete (NIDS)	Soluzioni di rilevamento delle intrusioni devono essere applicate alla rete dell'organizzazione.
C.C.6	Network Intrusion Prevention System (NIPS)	Soluzioni di prevenzione delle intrusioni devono essere applicate alla rete dell'organizzazione.
C.C.7	Controllo accessi alla rete mediante dispositivi mobili	L'accesso alla rete dell'organizzazione attraverso dispositivi mobili deve essere ristretto utilizzando tecnologie di Network Access Control (NAC), in grado di verificare la configurazione del dispositivo e gestire opportunamente l'accesso.
C.C.8	Hardening dei dispositivi di rete	I dispositivi di rete devono essere hardenizzati e configurati in maniera sicura
C.C.10	Network Level Authentication	Implementare l'autenticazione a livello rete mediante 802.1X al fine di limitare e controllare quali dispositivi possono accedere alla rete.
C.C.11	IP Tracking	Associazione IP/Host/Hostname per identificazione dei dispositivi in rete (necessario per Data Breach Management)
C.C.12	DNS Protection	Protezione dei server DNS per garantire la disponibilità della risoluzione dei nomi e quindi la possibilità di raggiungere l'applicazione
C.C.13	Zero Trust	Adozione di un modello di sicurezza "Zero Trust"