



**CLASSIFICAZIONE DEL DOCUMENTO: CONSIP PUBLIC**

**GARA A PROCEDURA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L’AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI**

**ACCORDO QUADRO PER L’AFFIDAMENTO SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI AI SENSI DELL’ART. ex art. 54, co. 4 lett. a) DEL d.lgs. N. 50/2016**

**LOTTO 2**

**ID SIGEF 2296**

Classificazione del documento: Consip Public

Accordo Quadro avente ad oggetto l’affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni - ID SIGEF 2296

Accordo Quadro Lotto 2



**SCHEMA DI ACCORDO QUADRO  
PER L’AFFIDAMENTO SERVIZI DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI**

**TRA**

**Consip S.p.A.**, a socio unico, con sede legale in Roma, Via Isonzo n. 19/E, capitale sociale Euro 5.200.000,00= i.v., iscritta al Registro delle Imprese presso la Camera di Commercio di Roma al n.REA 878407 di Roma, CF e P. IVA 05359681003, in persona dell’Amministratore Delegato e legale rappresentante, Ing. Cristiano Cannarsa, domiciliato per la carica presso la sede sociale, giusta poteri allo stesso conferiti dalla deliberazione di aggiudicazione del Consiglio di Amministrazione del 25/01/2022 (nel seguito per brevità anche “**Consip S.p.A.**”)

**E**

- **Deloitte Risk Advisory S.r.l. S.B.**, sede legale in Milano, Via Tortona n. 25, capitale sociale Euro 65.350,00=, iscritta al Registro delle Imprese di Milano al n. 050592500158, P. IVA 05059250158, domiciliata ai fini del presente atto in Milano, Via Tortona n.25, in persona del Procuratore e legale rappresentante Dott. Lorenzo Fersurella, nella sua qualità di impresa mandataria capo-gruppo del Raggruppamento Temporaneo oltre alla stessa le mandanti:

- **EY Advisory S.p.A.** con sede legale in Milano, Via Meravigli n.14, capitale sociale Euro 2.250.000,00=, iscritta al Registro delle Imprese di Milano al n. 13221390159, P. IVA 13221390159, domiciliata ai fini del presente atto in Milano, via Tortona n.25;

- **Teleco S.r.l.**, con sede legale in Roma, Via Rosazza n. 26, capitale sociale Euro 950.000,00=, iscritta al Registro delle Imprese di Milano al n. 02856220922, P. IVA 02856220922, domiciliata ai fini del presente atto in Milano, via Tortona n.25, giusta mandato collettivo speciale con rappresentanza autenticato dal notaio in Roma dott. Lorenzo Cavalaglio repertorio n. 14.339 del 3 febbraio 2022;

(nel seguito per brevità congiuntamente anche “**Fornitore**” o “**Impresa**”)

**PREMESSO**

- a)** l’art. 4, comma 3-quater, del D.L. n. 95/2012, come convertito con modificazioni dalla Legge n. 135/2012, ha stabilito che, per la realizzazione di quanto previsto dall’art. 20 del D.L. n. 83/2012, Consip S.p.A. svolge altresì le attività di centrale di committenza relativamente “ai contratti-quadro ai sensi dell’articolo 1, comma 192, della legge 30 dicembre 2004, n. 311”;
- b)** che l’articolo 2, comma 225, Legge 23 dicembre 2009, n. 191, consente a Consip S.p.A. di concludere Accordi Quadro a cui le Stazioni Appaltanti, possono fare ricorso per l’acquisto di beni e di servizi;
- c)** che, peraltro, l’utilizzazione dello strumento dell’Accordo Quadro e, quindi, una gestione in forma associata della procedura di scelta del contraente, mediante aggregazione della domanda di più soggetti, consente la razionalizzazione della spesa di beni e servizi, il supporto alla programmazione dei fabbisogni, la semplificazione e standardizzazione delle procedure di acquisto, il conseguimento di economie di scala, una maggiore trasparenza delle procedure di gara, il miglioramento della responsabilizzazione e del controllo della spesa, un incremento della specializzazione delle competenze, una maggiore efficienza nell’interazione fra Amministrazione e mercato e, non ultimo, un risparmio nelle spese di gestione della procedura medesima;
- d)** che in esecuzione di quanto precede, Consip S.p.A., in qualità di stazione appaltante e centrale di committenza, ha indetto con Bando di gara pubblicato nella Gazzetta Ufficiale della Repubblica Italiana n. 108 del 17/09/2021 e nella Gazzetta Ufficiale dell’Unione Europea n. S 178 del 14/09/2021, una procedura aperta per la stipula di un Accordo Quadro, ai sensi dell’art. 54, comma 4, lett. a) del D. Lgs. n. 50/2016 con più operatori a condizione tutte fissate;
- e)** il Fornitore che sottoscrive il presente Accordo Quadro è risultato aggiudicatario della predetta procedura aperta per la quota PAL del Lotto 2 e, per l’effetto, ha manifestato la volontà di impegnarsi ad eseguire quanto stabilito

Classificazione del documento: Consip Public

Accordo Quadro avente ad oggetto l’affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni - ID SIGEF 2296

Accordo Quadro Lotto 2



nel presente Accordo Quadro e relativi Allegati alle condizioni, modalità e termini ivi stabiliti e nei successivi Contratti esecutivi;

- f) che la stipula del presente Accordo Quadro con i suoi Allegati non è fonte di alcuna obbligazione per la Consip S.p.A. e/o per le Amministrazioni nei confronti del Fornitore;
- g) che i singoli Contratti esecutivi verranno stipulati a tutti gli effetti tra le Amministrazioni PAL secondo l'indicazione di cui al par. 5 del Capitolato Tecnico Generale ed il Fornitore in base alle modalità ed i termini indicati nel presente Accordo Quadro e relativi Allegati;
- h) che il Fornitore dichiara che quanto risulta dal presente Accordo Quadro e dai suoi Allegati, ivi compreso il Capitolato d'Oneri ed il Capitolato Tecnico (Generale e Speciale), nonché gli ulteriori atti della procedura, definisce in modo adeguato e completo gli impegni assunti con la firma del presente atto, nonché l'oggetto delle prestazioni da fornire e, in ogni caso, ha potuto acquisire tutti gli elementi per una idonea valutazione tecnica ed economica delle stesse e per la formulazione dell'offerta;
- i) il Fornitore ha presentato la documentazione richiesta ai fini della stipula del presente Accordo Quadro che, anche se non materialmente allegata al presente atto, ne forma parte integrante e sostanziale, ivi inclusa la garanzia definitiva nei confronti di Consip S.p.A., rilasciata dalla Euler Hermes ed avente n. 2565421 per un importo di Euro 400.000,00=(quattrocentomila/00) a garanzia dell'adempimento delle obbligazioni contrattuali nascenti dall'Accordo Quadro;
- j) che il Fornitore, con la seconda sottoscrizione, dichiara, ai sensi e per gli effetti di cui agli artt. 1341 e 1342 cod. civ., di accettare tutte le condizioni e patti contenuti nel presente Accordo Quadro e relativi Allegati, e di avere particolarmente considerato quanto stabilito e convenuto con le relative clausole; in particolare dichiara di approvare specificamente le clausole e condizioni riportate in calce al presente Accordo Quadro;
- k) che il presente Accordo Quadro viene sottoscritto dalle parti con firma digitale rilasciata da ente certificatore autorizzato;
- l) In data 25 febbraio 2022 è stato proposto dall'impresa NTT Data Italia S.p.A, innanzi al T.A.R. del Lazio, Roma, un giudizio iscritto al R.G. n. 2140/2022, contro Consip S.p.A e il RTI Deloitte Risk Advisory S.r.l. S.B., E&Y Advisory S.p.A., Teleco S.r.l. e nei confronti del RTI Intellera Consulting S.r.l., Cap Gemini Italia S.p.A., HSPI S.p.A. e Teleconsys S.p.A. per l'annullamento del provvedimento di aggiudicazione definitiva non efficace comunicato da Consip il 26/01/2022. Il Tar all'udienza camerale del 9/3/2022 non ha concesso misure cautelari ed in data 21/04/2022 ha pronunciato la sentenza n. 04840/2022 respingendo il gravame proposto da NTT Data Italia S.p.A..

***Ciò premesso, tra le parti come in epigrafe rappresentate e domiciliate***

**SI CONVIENE E SI STIPULA QUANTO SEGUE**

#### **ARTICOLO 1 - DEFINIZIONI**

1. Nell'ambito del presente Accordo Quadro, si intende per:

- a) **Accordo Quadro:** il presente atto, comprensivo di tutti i suoi Allegati, nonché dei documenti ivi richiamati, quale accordo concluso da Consip S.p.A. anche per conto delle Amministrazioni, da una parte, ed il Fornitore, dall'altra parte, con lo scopo di stabilire le clausole relative agli Contratti esecutivi da affidare per tutta la durata del medesimo Accordo Quadro;
- b) **Amministrazione/i o Amministrazione/i Contraente/i PAL:** le stazioni appaltanti, nonché gli altri soggetti che ai sensi della normativa vigente sono legittimati a affidare Contratti esecutivi basati sul presente Accordo Quadro secondo la classificazione di cui al par. 5 del Capitolato Tecnico Generale;
- m) **Ministero:** Ministero dell'Economia e delle Finanze;

Classificazione del documento: Consip Public

Accordo Quadro avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni - ID SIGEF 2296

Accordo Quadro Lotto 2



- c) **Data di Attivazione:** la data a partire dalla quale le Amministrazioni Pubbliche possono utilizzare l'Accordo Quadro, ai sensi di quanto disposto nel successivo art. 4;
  - d) **Fornitore:** il singolo aggiudicatario (impresa, raggruppamento temporaneo o consorzio di imprese) della procedura aperta di cui in premessa, che, conseguentemente, sottoscrive l'Accordo Quadro impegnandosi a quanto nello stesso previsto e, in particolare, ad eseguire i singoli Contratti esecutivi;
  - e) **Capitolato d'Oneri:** il documento allegato al presente atto che ha disciplinato la partecipazione alla procedura aperta di cui in premessa, e contenente, altresì, le condizioni e le modalità per l'affidamento dei Contratti esecutivi;
  - f) **Contratto esecutivo:** il Contratto che si perfeziona in seguito della decorrenza del termine di 4 giorni lavorativi dalla ricezione del Piano operativo da parte dell'operatore economico, individuato, tra gli aggiudicatari dell'Accordo Quadro, avente ad oggetto l'affidamento di servizi di compliance e controllo, in base ai criteri, le modalità ed i termini indicati nel presente Accordo Quadro e nel paragrafo 6.5 del Capitolato Tecnico Generale;
  - g) **Piano dei Fabbisogni:** il documento inviato dall'Amministrazione al Fornitore, con il la stessa identifica e contestualizza i servizi oggetto del proprio Contratto esecutivo e nel quale dovranno essere riportate, tra le altre cose, le specifiche esigenze dell'Amministrazione che hanno portato alla scelta del fornitore;
  - h) **Piano operativo:** il documento, inviato dal Fornitore all'Amministrazione, contenente la traduzione operativa dei fabbisogni espressi dall'Amministrazione con le modalità indicate nel Capitolato Tecnico Generale;
  - i) **Giorno lavorativo:** da lunedì a sabato, esclusi domenica e festivi;
  - j) **Soggetti aggregatori:** le centrali di committenza iscritte nell'elenco istituito ai sensi dell'art. 9, comma 1, del decreto legge 24 aprile 2014, n. 66, convertito con modificazioni, dalla legge 23 giugno 2014, n. 89, come definiti all'art. 3, comma 1, lett. n) del D.Lgs. n. 50/2016.
2. Le espressioni riportate negli Allegati al presente Accordo Quadro hanno il significato, per ognuna di esse, specificato nei medesimi Allegati, tranne qualora il contesto delle singole clausole dell'Accordo Quadro disponga diversamente.

## ARTICOLO 2 - VALORE DELLE PREMESSE, DEGLI ALLEGATI E NORME REGOLATRICI

1. Le premesse di cui sopra, gli atti ed i documenti richiamati nelle medesime premesse e nella restante parte del presente atto, ivi incluso il Bando di gara, il Capitolato d'Oneri, il Capitolato Tecnico Generale e Speciale e le relative appendici, i chiarimenti resi in fase di gara, le Regole del Sistema di e-Procurement della Pubblica Amministrazione – Parte I, ancorché non materialmente allegati, costituiscono parte integrante e sostanziale del presente Accordo Quadro. Tali documenti sono disponibili al seguente link: [www.consip.it](http://www.consip.it).
2. Costituiscono, altresì, parte integrante e sostanziale dell'Accordo Quadro: l'Allegato "A" (Offerta Tecnica del Fornitore), Allegato "B" (Offerta Economica del Fornitore) Allegato "C" (Corrispettivi e tariffe PAL) Allegato "D" (Patto di integrità), l'Allegato "E" (Nomina a responsabile del trattamento dei dati), l'Allegato "F" (Schema di contratto esecutivo – Lotto 2), l'Allegato "G" (Disposizioni per la Governance), l'Allegato "H" (Regolamento degli organismi di coordinamento e controllo), l'Allegato "I" (Contratto di fornitura continuativa),.
3. Il presente Accordo Quadro è regolato:
  - a) dal contenuto dell'Accordo Quadro e dei suoi Allegati che costituiscono la manifestazione integrale di tutti gli accordi intervenuti con il Fornitore relativamente alle attività e prestazioni contrattuali che costituiscono parte integrante e sostanziale dell'Accordo Quadro;
  - b) dalle disposizioni di cui al D.Lgs. n. 50/2016 e s.m.i.;
  - c) dalle disposizioni di cui al d.P.R. 10 ottobre 2010, n. 207, nei limiti stabiliti dagli artt. 216 e 217 del D. Lgs. n. 50/2016;
  - d) dalle disposizioni anche regolamentari in vigore per le Amministrazioni, di cui il Fornitore dichiara di avere esatta conoscenza e che, sebbene non siano materialmente allegati, formano parte integrante del presente atto;

Classificazione del documento: Consip Public

Accordo Quadro avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni - ID SIGEF 2296

Accordo Quadro Lotto 2





- e) dalle norme in materia di Contabilità pubblica;
  - f) dal codice civile e dalle altre disposizioni normative in vigore in materia di contratti di diritto privato;
  - g) dal Codice Etico e dal Piano Triennale per la prevenzione della corruzione e della trasparenza della Consip S.p.A., consultabili sul sito internet della stessa Consip;
  - h) dal patto di integrità.
4. I Contratti esecutivi saranno regolati, dalle disposizioni in essi previste, dal presente Accordo Quadro e dai suoi allegati, dalle disposizioni indicate al precedente comma.
5. In caso di contrasto o difficoltà interpretativa tra quanto contenuto nel presente Accordo Quadro e relativi Allegati, da una parte, e quanto dichiarato nell'Offerta Tecnica, dall'altra parte, prevarrà quanto contenuto nei primi, fatto comunque salvo il caso in cui l'Offerta Tecnica contenga, a giudizio di Consip S.p.A. e/o delle Amministrazioni, previsioni migliorative rispetto a quelle contenute nel presente Accordo Quadro e relativi Allegati.
6. Le clausole dell'Accordo Quadro e dei Contratti esecutivi sono sostituite, modificate od abrogate automaticamente per effetto di norme aventi carattere cogente contenute in leggi o regolamenti che entreranno in vigore successivamente, fermo restando che in ogni caso, anche ove intervengano modificazioni autoritative dei prezzi migliorativi per il Fornitore, quest'ultimo rinuncia a promuovere azioni o ad opporre eccezioni rivolte a sospendere o a risolvere il rapporto contrattuale in essere.
7. Nel caso in cui dovessero sopraggiungere provvedimenti di pubbliche autorità dai contenuti non suscettibili di inserimento di diritto nel presente Accordo Quadro e nei Contratti esecutivi e che fossero parzialmente o totalmente incompatibili con l'Accordo Quadro e relativi Allegati e/o con i Contratti esecutivi, Consip S.p.A. e/o le Amministrazioni, da un lato, e il Fornitore, dall'altro lato, potranno concordare le opportune modifiche ai surrichiamati documenti sul presupposto di un equo temperamento dei rispettivi interessi e nel rispetto dei relativi criteri di aggiudicazione della procedura.

### **ARTICOLO 3 - OGGETTO DELL'ACCORDO QUADRO**

1. L'Accordo Quadro definisce la disciplina normativa e contrattuale relativa alle condizioni e alle modalità di affidamento da parte delle Amministrazioni dei singoli Contratti esecutivi aventi ad oggetto l'affidamento di servizi di compliance e controllo (Lotto 2 PAL) alle condizioni tutte espressamente stabilite nel presente atto e relativi Allegati.

Il valore indicativo stimato dell'Accordo Quadro, rappresentativo della sommatoria dell'importo massimo presunto dei Contratti esecutivi che verranno affidati in virtù dell'Accordo Quadro medesimo, è il seguente: Euro 117.000.000,00 = (centodiciassettemilioni) IVA esclusa, come di seguito suddiviso:

- attribuzione della quota massima del valore di Euro 70.200.000,00 = (settantamilioniduecentomila), IVA esclusa, al Fornitore graduato primo nella graduatoria di merito.
2. Qualora, anteriormente alla scadenza del termine di durata dell'Accordo Quadro, anche eventualmente prorogata, il valore relativo ad un Contratto esecutivo raggiunga il valore stimato dell'Accordo Quadro medesimo oppure lo ecceda (comunque fino a una soglia massima del 20%), Consip considererà quest'ultimo come giunto a scadenza e di conseguenza non potranno essere affidati ulteriori Contratti esecutivi. La regola sopra illustrata opera sul massimale della quota di AQ stipulato con il Fornitore.
3. Il presente Accordo Quadro è concluso con il Fornitore aggiudicatario della procedura aperta di cui in premessa, il quale con la sottoscrizione del presente atto, si impegna a dare esecuzione ai Contratti esecutivi che si perfezioneranno all'esito dell'approvazione del Piano operativo, quale affidamento in favore del Fornitore del Contratto esecutivo basato sulle condizioni stabilite nel presente Accordo Quadro e relativi Allegati.
4. L'affidamento del Contratto esecutivo da parte della singola Amministrazione avverrà in favore del Fornitore che

Classificazione del documento: Consip Public

Accordo Quadro avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni - ID SIGEF 2296

Accordo Quadro Lotto 2



sottoscrive il presente contratto in ragione del fatto che la medesima appartiene alla PAL come indicato al capitolo 5 del Capitolato Tecnico Generale.

5. Il Fornitore, pertanto, si impegna ad eseguire, in caso di affidamento dei singoli Contratti esecutivi, i servizi di compliance e controllo descritti nel Capitolato Tecnico Speciale (Lotto 2) secondo quanto ivi stabilito e nel rispetto delle condizioni di erogazione migliorative eventualmente offerte in sede di gara, nonché, in ogni caso nel rispetto di quanto stabilito nel Capitolato d'oneri, nel Capitolato Tecnico (Generale e Speciale) e negli atti della documentazione di gara, ovvero se migliorative, nell'Offerta Tecnica allegata.
6. Al fine di affidare un Contratto esecutivo basato sul presente Accordo Quadro, le singole Amministrazioni procedono:
  - a) alla definizione dell'oggetto del singolo Contratto esecutivo, del quantitativo e dell'importo contrattuale, nel rispetto di quanto stabilito ed alle condizioni di cui al presente Accordo Quadro e relativi Allegati e comunque di quanto previsto al paragrafo 6.5 del Capitolato Tecnico Generale;
  - b) *<qualora l'Amministrazione Contraente ricada tra i soggetti di cui all'art. 1, comma 2, lett. a) della legge n. 133/2019 e l'oggetto del proprio Contratto esecutivo sia destinato a essere impiegato sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui all'art. 1, comma 2, lettera b), della legge n. 133/2019>* alla comunicazione al CVCN o a uno dei CV secondo quanto previsto dall'art. 1 comma 6, legge n. 133/2019 la cui efficacia è stata modificata dall'art 16 comma 9, lett. a) della Legge n. 109/2021 secondo quanto previsto dall'art. 1 comma 6, legge n. 133/2019;
  - c) all'affidamento del Contratto esecutivo in favore del Fornitore approvando il Piano Operativo nel rispetto delle condizioni previste nel presente Accordo Quadro e relativi Allegati, e al conseguente perfezionamento del relativo Contratto Esecutivo.

#### **ARTICOLO 4 - DURATA DELL'ACCORDO QUADRO E DEI CONTRATTI ESECUTIVI**

1. Il presente Accordo Quadro ha una durata di 24 mesi a decorrere dalla data di attivazione, ovvero la minore durata determinata dall'esaurimento del valore massimo stabilito nel precedente articolo.
2. Resta inteso che, per durata dell'Accordo Quadro, si intende il termine entro il quale le Amministrazioni potranno affidare i singoli Contratti esecutivi al Fornitore per l'approvvigionamento dei servizi oggetto dell'Accordo Quadro stesso.
3. Ciascun Contratto esecutivo ha una durata massima di 48 mesi, decorrenti dalla data di conclusione delle attività di presa in carico.
4. L'Amministrazione, in conformità a quanto disposto all'articolo 106, comma 11, del D. Lgs. n. 50/2016, si riserva la facoltà in corso di esecuzione di modificare la durata del contratto, con comunicazione inviata a mezzo pec al Fornitore, prorogandolo per il tempo strettamente necessario alla conclusione delle procedure necessarie per l'individuazione di un nuovo contraente, ivi inclusa la stipula del contratto. In tal caso il Fornitore è tenuto all'esecuzione delle prestazioni previste nel contratto agli stessi prezzi, patti e condizioni o più favorevoli per l'Amministrazione.

#### **ARTICOLO 5 - PREZZI E VINCOLI DEI CONTRATTI ESECUTIVI**

1. I corrispettivi per ciascun Contratto esecutivo verranno determinati sulla base dei prezzi stabiliti nell'Allegato "C", "Corrispettivi e tariffe PAL", i quali rappresentano quindi un vincolo per il Fornitore.
2. Il Fornitore, inoltre, nel dare seguito al singolo Contratto esecutivo dovrà, fermi i prezzi unitari offerti, fornire servizi che dovranno necessariamente possedere tutte le caratteristiche (minime e migliorative offerte) per

Classificazione del documento: Consip Public

Accordo Quadro avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni - ID SIGEF 2296

Accordo Quadro Lotto 2



l'aggiudicazione del presente Accordo Quadro.

3. Il pagamento dei corrispettivi dovrà essere effettuato mediante strumenti di pagamento idonei a consentire la piena tracciabilità delle operazioni ai sensi della Legge 13 agosto 2010 n. 136 e s.m.i., del Decreto Legge 12 novembre 2010 n. 187 nonché ai sensi delle emanate Determinazioni dell'A.N.AC., e, fatte salve le eventuali ulteriori indicazioni sugli "strumenti idonei" che dovessero essere emanate dalla medesima Autorità.
4. La disciplina della revisione dei corrispettivi dovuti al Fornitore sarà definita dalle Amministrazioni in sede di Contratto esecutivo, fermo restando quanto previsto all'art. 106 comma1 del D. Lgs. 50/2016.

#### **ARTICOLO 6 - AFFIDAMENTO DEI CONTRATTI ESECUTIVI**

1. Ciascun Contratto esecutivo verrà affidato dalla singola Amministrazione nel rispetto e alle condizioni stabilite al paragrafo 6.5 del capitolato Tecnico Generale, al paragrafo 24 del Capitolato d'Oneri e agli artt. 3 e 4 del presente atto.
2. Sono legittimate ad utilizzare il presente Accordo Quadro, ai sensi della normativa vigente, le Amministrazioni PAL come definite nel precedente articolo 1 e sulla base di quanto indicato al capitolo 5 del Capitolato Tecnico Generale ("Razionali per l'utilizzo dei Lotti"). Ove il Fornitore ritenga di non poter dare seguito al Contratto esecutivo, in quanto proveniente da un soggetto non legittimato sulla base di quanto sopra, dovrà, tempestivamente e comunque entro il termine stabilito al paragrafo 6.5.2. del Capitolato Tecnico Generale, informare Amministrazione e Consip, spiegando le ragioni del rifiuto.
3. All'esito della procedura di cui al paragrafo 6.5 del Capitolato Tecnico Generale, l'Amministrazione invierà a mezzo PEC al Fornitore il Piano operativo approvato ed il Contratto esecutivo sottoscritto.
4. Qualora il Fornitore rilevi eventuali difformità, nell'ambito del Contratto esecutivo, rispetto alle previsioni di cui al presente Accordo Quadro e relativi allegati e al Capitolato Tecnico Generale, ovvero la mancanza degli elementi essenziali dello schema di Contratto esecutivo, dovrà darne tempestiva comunicazione all'Amministrazione, entro e non oltre quattro giorni lavorativi dal ricevimento del Contratto esecutivo stesso. In tal caso, l'Amministrazione potrà trasmettere nuovamente il Contratto esecutivo, conforme alle previsioni di cui all'Accordo Quadro e relativi allegati.
5. In assenza di comunicazioni ai sensi del precedente comma 4, il singolo Contratto esecutivo si perfezionerà in ogni caso il quarto giorno lavorativo successivo alla trasmissione, da parte dell'Amministrazione, del Contratto esecutivo dalla stessa sottoscritto. Spirato il predetto termine, nonché in caso di accettazione espressa, il Fornitore sarà pertanto tenuto a dare esecuzione completa alla fornitura richiesta. Il ritardo nell'avvio dell'esecuzione per causa imputabile al Fornitore costituisce causa di risoluzione di diritto del Contratto esecutivo, ai sensi dell'art. 2, comma 1 della L. n. 120/2020 DL. 76/2020.
6. Per effetto del perfezionamento del Contratto esecutivo, il Fornitore sarà obbligato ad eseguire la fornitura richiesta, nell'ambito dell'oggetto contrattuale, restando inteso che in caso di mancata utilizzazione dell'Accordo Quadro da parte dei soggetti sopra indicati nulla potrà essere preteso a qualsiasi titolo dal medesimo Fornitore il quale, infatti, sarà tenuto a svolgere le attività, effettuare le forniture e prestare i servizi solo a seguito del perfezionamento dei Contratti esecutivi, con le modalità ed in conformità alle condizioni sopra indicate.
7. Resta inteso che Consip non potrà in alcun modo essere ritenuta responsabile per il mancato perfezionamento dei Contratti esecutivi da parte delle Amministrazioni ed inoltre resta fermo che non sussiste in capo a Consip alcuna verifica dei poteri di acquisto attribuiti al sottoscrittore del Contratto esecutivo.
8. Qualora il Fornitore non abbia autorizzato Consip alla pubblicazione delle generalità e del codice fiscale del/i delegato/i ad operare sul conto/i corrente/i dedicato/i, il Fornitore medesimo sarà tenuto a comunicare, entro e non oltre due giorni dal perfezionamento del singolo Contratto esecutivo i surrichiamati dati alle Amministrazioni Contraenti.

Classificazione del documento: Consip Public



9. Qualora venga richiesto da Consip, il Fornitore, entro un giorno lavorativo dalla richiesta, ha l'obbligo di dare riscontro alla medesima Consip, anche per via telematica, di ciascun Contratto esecutivo perfezionato.
10. Le Amministrazioni provvederanno, prima della sottoscrizione del singolo Contratto esecutivo, tra le altre cose: i) alla nomina del Responsabile del Procedimento, ai sensi e per gli effetti dell'art. 31 del D.Lgs. n. 50/2016 ii) alla nomina del Direttore dell'esecuzione, laddove le relative funzioni non siano svolte dal Responsabile del procedimento nel rispetto degli artt. 101, 102 e 111 del D.Lgs. n. 50/2016; iii) ai sensi e per gli effetti dell'art. 3 della Legge 13 agosto 2010 n. 136 e s.m.i., degli artt. 6 e 7 del Decreto Legge 12 novembre 2010, n. 187 nonché della Determinazione dell'Autorità per la Vigilanza sui Contratti Pubblici (ora A.N.AC.) n. 8 del 18 novembre 2010, alla indicazione sul medesimo Contratto esecutivo del CIG (Codice Identificativo Gara) "derivato" rispetto a quello dell'Accordo Quadro e da esse richiesto nonché del CUP (Codice Unico Progetto) ove obbligatorio ai sensi dell'art. 11 della Legge 16 gennaio 2003 n. 3.
11. Le Amministrazioni provvederanno, ove ritenuto necessario, alla nomina del Fornitore quale Responsabile o sub Responsabile del trattamento dei dati personali, eventualmente utilizzando l'Allegato Privacy, accluso al presente Accordo Quadro.
12. Resta salva la facoltà per Consip S.p.A. di svolgere controlli sull'esecuzione delle singole prestazioni.
13. Nel caso di Contratto esecutivo affidato da un Soggetto Aggregatore, nel Progetto dei fabbisogni il Soggetto Aggregatore, inoltre:
  - dovrà indicare tutte le singole Amministrazioni per le quali il Soggetto Aggregatore effettua l'affidamento;
  - dovrà indicare gli importi e i quantitativi relativi ad ogni singola Amministrazione;
  - potrà indicare le eventuali modalità di ripartizione degli obblighi di fatturazione tra il Soggetto Aggregatore e le singole Amministrazioni.
14. Il Fornitore prende atto, rinunciando ora per allora a qualsiasi pretesa di risarcimento o di indennizzo, che l'Amministrazione ha la facoltà di revocare il Piano dei Fabbisogni, da esercitarsi entro un giorno lavorativo dall'emissione del medesimo.
15. Le Amministrazioni possono, nei limiti di quanto previsto all'art. 106, comma 7, del D. Lgs. n. 50/2016, chiedere al Fornitore prestazioni supplementari rispetto al Contratto esecutivo, che si rendano necessarie, ove un cambiamento del contraente produca entrambi gli effetti di cui all'art. 106, comma 1, lettera b), D. Lgs. n. 50/2016; l'Amministrazione comunicherà ad ANAC tale modifica entro i termini di cui all'art. 106, comma 8, del medesimo decreto.
16. Le Amministrazioni possono apportare modifiche al contratto esecutivo ove siano soddisfatte tutte le condizioni di cui all'art. 106, comma 1, lettera c), D. Lgs. 50/2016, fatto salvo quanto previsto all'art. 106, comma 7, del D. Lgs. n. 50/2016. Al ricorrere delle condizioni di cui all'art. 106, comma 14, del D. Lgs. 50/2016 l'Amministrazione comunicherà ad ANAC tale modifica entro i termini e con le modalità ivi indicati. In entrambi i casi sopra descritti, l'Amministrazione eseguirà le pubblicazioni prescritte dall'art. 106, comma 5, del D. Lgs. n. 50/2016.
17. Le Amministrazioni potranno apportare le modifiche di cui art. 106, comma 1, lett. d), del D. Lgs. n. 50/2016, nel pieno rispetto di tale previsione normativa.
18. Così come chiarito dal **Comunicato Anac del 23 marzo 2021**, l'Amministrazione potrà imporre al fornitore affidatario dell'Appalto Specifico un aumento o una diminuzione delle prestazioni fino a concorrenza di un quinto dell'importo del contratto alle stesse condizioni ed agli stessi prezzi unitari previsti dal presente Contratto, solo laddove ricorrano i presupposti di cui al **combinato disposto dei commi 1, lett. c) e 12 dell'art. 106, del Codice**. In tal caso, il Fornitore non può far valere il diritto alla risoluzione del contratto.
19. Per tutto quanto non espressamente previsto nel presente articolo, si applicano le disposizioni di cui all'art. 106 del D.Lgs. 50/2016.

Classificazione del documento: Consip Public

Accordo Quadro avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni - ID SIGEF 2296

Accordo Quadro Lotto 2



20. Nel corso dell'esecuzione del Contratto esecutivo, l'Amministrazione potrà richiedere aggiornamenti del Piano dei Fabbisogni e del Piano Operativo ogni qualvolta lo ritenga necessario, nel rispetto delle previsioni di cui all'art. 106 del D.Lgs. 50/2016 nonché dell'importo massimo dell'Accordo Quadro.
21. Qualora l'Amministrazione Contraente ricada tra i soggetti di cui all'art. 1, comma 2, lett. a) della legge n. 133/2019 e l'oggetto del proprio Contratto esecutivo sia destinato a essere impiegato sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui all'art. 1, comma 2, lettera b), della legge n. 133/2019, atteso che prima di procedere all'affidamento del Contratto esecutivo, il Centro di valutazione e certificazione nazionale (CVCN), istituito presso il Ministero dello sviluppo economico e trasferito dal D.L. 82/2021 (convertito con modificazioni dalla L. 109/2021) presso l'Agenzia per la cybersicurezza nazionale, o uno dei Centri di Valutazione (CV), istituiti presso il Ministero dell'interno e il Ministero della difesa, potrà aver riscontrato la comunicazione della medesima prevedendo la necessità di effettuare verifiche preliminari e/o imporre condizioni e test hardware e software su forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui al comma 2 lett. b) legge 133/2019, l'Amministrazione contraente prevedrà nel Contratto esecutivo medesimo le clausole che condizioneranno, sospensivamente ovvero risolutivamente al Contratto esecutivo al rispetto delle condizioni e all'esito favorevole dei test disposti dal CVCN.

#### **ARTICOLO 7 - OBBLIGAZIONI GENERALI DEL FORNITORE**

1. Sono a carico del Fornitore tutti gli oneri e rischi relativi alla prestazione delle attività oggetto dei Contratti esecutivi basati sul presente Accordo Quadro, nonché ad ogni attività che si rendesse necessaria per l'attivazione e la prestazione degli stessi o, comunque, opportuna per un corretto e completo adempimento delle obbligazioni previste, ivi compresi quelli relativi ad eventuali spese di trasporto, di viaggio e di missione per il personale addetto alla esecuzione contrattuale.
2. Il Fornitore si obbliga ad eseguire tutte le prestazioni a perfetta regola d'arte, nel rispetto delle norme vigenti e secondo le condizioni, le modalità, i termini e le prescrizioni contenute nell'Accordo Quadro, nel Capitolato d'Oneri, nel Capitolato Tecnico Generale e Speciale, nel Piano dei fabbisogni, nel Piano Operativo, ivi inclusi i rispettivi Allegati.
3. Le prestazioni contrattuali dovranno necessariamente essere conformi alle caratteristiche tecniche e qualitative eventualmente migliorate in Offerta tecnica ed alle specifiche indicate nel Capitolato d'Oneri e nei relativi Allegati; in ogni caso, il Fornitore si obbliga ad osservare, nell'esecuzione delle prestazioni contrattuali, tutte le norme e le prescrizioni tecniche e di sicurezza in vigore, nonché quelle che dovessero essere successivamente emanate.
4. Gli eventuali maggiori oneri derivanti dalla necessità di osservare le norme e le prescrizioni di cui sopra, anche se entrate in vigore successivamente alla stipula dell'Accordo Quadro, resteranno ad esclusivo carico del Fornitore, intendendosi in ogni caso remunerati con il corrispettivo contrattuale indicato nel Contratto esecutivo, ed il Fornitore non potrà, pertanto, avanzare pretesa di compensi a tale titolo, nei confronti delle Amministrazioni e/o della Consip S.p.A., assumendosene ogni relativa alea.
5. Il Fornitore si impegna espressamente a:
  - a) impiegare, a proprie cura e spese, tutte le strutture ed il personale necessario per l'esecuzione dei Contratti esecutivi secondo quanto specificato nell'Accordo Quadro e nei rispettivi Allegati e negli atti di gara richiamati nelle premesse;
  - b) rispettare, per quanto applicabili, le norme internazionali UNI EN ISO vigenti per la gestione e l'assicurazione della qualità delle proprie prestazioni;
  - c) predisporre tutti gli strumenti e i metodi, comprensivi della relativa documentazione, atti a consentire alla Consip

Classificazione del documento: Consip Public



S.p.A. e alle singole Amministrazioni, per quanto di propria competenza, di monitorare la conformità dei servizi e delle forniture alle norme previste nell'Accordo Quadro e nei Contratti esecutivi fra i quali:

- i) l'invio entro il decimo giorno del mese successivo a quello di riferimento, dell'archivio in formato xml "FLUSSO DATI" recante i dati dei Contratti Esecutivi stipulati nel mese di riferimento;
  - ii) l'Invio entro il 31 gennaio del 2023, 2024 e 2025, della relazione consuntiva "FATTURATO ANNUALE" contenente, per servizio e per Amministrazione, le quantità di servizi erogati, il fatturato e le penali applicate relativo all'anno precedente.
- d) predisporre tutti gli strumenti e i metodi, comprensivi della relativa documentazione, atti a garantire elevati livelli di servizio, ivi compresi quelli relativi alla sicurezza e riservatezza;
  - e) nell'adempimento delle proprie prestazioni ed obbligazioni, osservare tutte le indicazioni operative, di indirizzo e di controllo che a tale scopo saranno predisposte e comunicate dalle Amministrazioni o dalla Consip S.p.A., per quanto di rispettiva ragione;
  - f) comunicare tempestivamente a Consip S.p.A. e alle Amministrazioni, per quanto di rispettiva competenza, le eventuali variazioni della propria struttura organizzativa coinvolta nell'esecuzione dell'Accordo Quadro e nei singoli Contratti esecutivi, indicando analiticamente le variazioni intervenute ed i nominativi dei nuovi responsabili;
  - g) non opporre a Consip S.p.A. e alle Amministrazioni qualsivoglia eccezione, contestazione e pretesa relative alla fornitura e/o alla prestazione dei servizi;
  - h) manlevare e tenere indenne Consip S.p.A. e le Amministrazioni da tutte le conseguenze derivanti dalla eventuale inosservanza delle norme e prescrizioni tecniche, di sicurezza, di igiene e sanitarie vigenti;
  - i) adottare, in fase di esecuzione contrattuale, le eventuali cautele rese necessarie dallo svolgimento delle prestazioni affidate in locali o ambienti in cui l'Amministrazione Contraente tratta informazioni classificate, con particolare riguardo alle specifiche misure previste dalla normativa in proposito vigente;
  - j) rispettare gli obblighi in materia ambientale, sociale e del lavoro stabiliti dalla normativa europea e nazionale, dai contratti collettivi o dalle disposizioni internazionali elencate nell'allegato X del D. Lgs. n. 50/2016.
  - k) ad effettuare le verifiche preliminari richieste dal CVCN nonché a rispettare le condizioni e i test hardware e software su forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui al comma 2 lett. b) legge 133/2019 eventualmente imposti dal CVCN.
6. Le attività necessarie per la predisposizione dei mezzi e per l'attivazione dei servizi oggetto dell'Accordo Quadro e dei singoli Contratti esecutivi, eventualmente da svolgersi presso gli uffici delle Amministrazioni, dovranno essere eseguite senza interferire nel normale lavoro degli uffici; modalità e tempi dovranno comunque essere concordati con le Amministrazioni stesse nel rispetto di quanto stabilito nel Capitolato Tecnico Generale e Speciale; peraltro, il Fornitore prende atto che, nel corso dell'esecuzione delle prestazioni contrattuali, gli uffici delle Amministrazioni continueranno ad essere utilizzati dal personale delle Amministrazioni stesse e/o da terzi autorizzati. Il Fornitore si impegna, pertanto, ad eseguire le predette prestazioni salvaguardando le esigenze delle Amministrazioni e/o di terzi autorizzati, senza recare intralci, disturbi o interruzioni alla attività lavorativa in atto.
7. Il Fornitore rinuncia espressamente, ora per allora, a qualsiasi pretesa o richiesta di compenso nel caso in cui l'esecuzione delle prestazioni contrattuali dovesse essere ostacolata o resa più onerosa dalle attività svolte dalle Amministrazioni e/o da terzi autorizzati.
8. Il Fornitore si impegna ad avvalersi di personale specializzato, in relazione alle diverse prestazioni contrattuali; detto personale potrà accedere agli uffici delle Amministrazioni nel rispetto di tutte le relative prescrizioni di accesso, fermo restando che sarà cura ed onere del Fornitore verificare preventivamente tali procedure.

Classificazione del documento: Consip Public



9. Il Fornitore si obbliga a: (a) dare immediata comunicazione a Consip S.p.A. e alle singole Amministrazioni, di ogni circostanza che abbia influenza sull'esecuzione delle attività di cui all'Accordo Quadro e ai singoli Contratti esecutivi; (b) prestare i servizi nei luoghi che verranno indicati nei Contratti esecutivi stessi.
10. Il Fornitore prende atto ed accetta che i servizi oggetto dell'Accordo Quadro dovranno essere prestati con continuità anche in caso di eventuali variazioni della consistenza e della dislocazione delle sedi e degli uffici delle Amministrazioni.
11. Nel rispetto della normativa vigente i servizi oggetto dell'Accordo Quadro e dei singoli Contratti esecutivi non sono affidati al Fornitore in via esclusiva, pertanto le Amministrazioni possono affidare le stesse forniture, attività e servizi anche a soggetti terzi, diversi dal medesimo Fornitore.
12. Il Fornitore è tenuto a comunicare a Consip S.p.A. e alle altre Amministrazione ogni modificazione negli assetti proprietari, nella struttura di impresa e negli organismi tecnici e amministrativi. Tale comunicazione dovrà pervenire a Consip S.p.A. entro 15 (quindici) giorni dall'intervenuta modifica.
13. Ai sensi dell'art. 105, comma 2, D.Lgs. n. 50/2016, con riferimento a tutti i sub-contratti stipulati dal Fornitore per l'esecuzione del contratto, è fatto obbligo al Fornitore stesso di comunicare, a Consip S.p.A. e all'Amministrazione interessata, il nome del sub-contraente, l'importo del contratto, l'oggetto delle attività, delle forniture e dei servizi affidati. Eventuali modifiche a tali informazioni avvenute nel corso del sub-contratto dovranno essere altresì comunicate a Consip S.p.A. e all'Amministrazione interessata.
14. Si precisa che le attività di coordinamento del presente AQ verranno svolte con il supporto dell'Organismo di Coordinamento e Controllo di cui al Capitolato Tecnico parte generale.
15. Ai sensi dell'art. 47 comma 3bis, della L. n. 108/2021, il Fornitore è tenuto a consegnare alla Committente in relazione a ciascuna impresa e/o consorziata che occupa un numero pari o superiore a quindici dipendenti e che non rientra nella classificazione di cui all'art. 46 comma 1, del d.lgs. n. 198/2006:
  - la certificazione di cui all'articolo 17 della legge 12 marzo 1999, n. 68;
  - una relazione relativa all'assolvimento degli obblighi di cui alla medesima legge n. 68/1999 e alle eventuali sanzioni e provvedimenti disposti a loro carico nel triennio antecedente la data di scadenza di presentazione delle offerte. La relazione dovrà essere trasmessa anche alle rappresentanze sindacali aziendali.

La documentazione di cui sopra, corredata dall'attestazione dell'avvenuta trasmissione della relazione alle rappresentanze sindacali aziendali, dovrà essere consegnata alla Consip, **entro 6 mesi dalla stipula** dell'Accordo Quadro.

La violazione anche di uno solo di tali obblighi comporta l'applicazione delle penali di cui al successivo articolo "Penali".

16. La relazione di cui al precedente comma 15 sarà pubblicata sul profilo del Committente, nella sezione "Amministrazione trasparente", ai sensi dell'art. 29, comma 1 del Codice e dell'art. 47, comma 9, della L. n. 108/2021. La Committente procederà anche con gli ulteriori adempimenti di cui al citato articolo 47 comma 9, della L. n. 108/2021.

#### **ARTICOLO 7BIS S CONTRATTI CONTINUATIVI DI COOPERAZIONE, SERVIZIO E/O FORNITURA**

Il Fornitore ricorre alle seguenti prestazioni di soggetti terzi, conformemente a quanto dichiarato in dichiarazione aggiuntiva e in forza dei contratti continuativi di cooperazione, servizio e/o fornitura, di cui al comma 3, lettera c-bis), dell'art. 105 del Codice, sottoscritti in epoca anteriore all'indizione della presente procedura, prodotti in sede di stipula del presente contratto.

Le prestazioni di soggetti terzi rese in virtù di contratti di cui al comma 3, lettera c-bis), dell'art. 105 del Codice, sottoscritti in epoca anteriore all'indizione della procedura finalizzata all'aggiudicazione del contratto e consegnati

Classificazione del documento: Consip Public

Accordo Quadro avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni - ID SIGEF 2296

Accordo Quadro Lotto 2





alla Committente prima o contestualmente alla sottoscrizione del Contratto, non costituiscono subappalto.

#### **ARTICOLO 8 - OBBLIGAZIONI SPECIFICHE DEL FORNITORE**

1. Il Fornitore dell'Accordo Quadro ha l'obbligo di tenere costantemente aggiornata, per tutta la durata del presente Accordo Quadro, la documentazione amministrativa richiesta e presentata a Consip S.p.A. per la stipula del presente Accordo Quadro. In particolare, pena l'applicazione delle penali di cui oltre, ciascun Fornitore ha l'obbligo di:
  - a) comunicare, entro 15 (quindici) giorni dall'intervenuta modifica e/o integrazione, ogni modificazione e/o integrazione relativa al possesso dei requisiti di cui al paragrafo III.1.1 del Bando di gara;
  - b) comunicare, entro 15 (quindici) giorni dalle intervenute modifiche, le modifiche soggettive di cui all'art. 80 del D.Lgs. n. 50/2016;
  - c) comunicare alla Consip S.p.A. ogni modifica o il venir meno dei requisiti attestanti la capacità tecnica richiesta (Certificazioni ISO 9001) ai fini della partecipazione, entro il termine perentorio di 15 (quindici) giorni lavorativi decorrenti dall'evento modificativo.
2. Il Fornitore in adempimento di quanto previsto dall' articolo 22 del Regolamento UE/2021/241 del 12 febbraio 2021, in tema di tutela degli interessi finanziari dell'Unione Europea, ha dichiarato i dati identificativi dei titolari effettivi, anche eventualmente schermati da società fiduciarie.

#### **ARTICOLO 9 - VERIFICA DI CONFORMITÀ**

1. Con riferimento al singolo Contratto esecutivo, ciascuna Amministrazione Contraente procederà ad effettuare la verifica di conformità dei servizi oggetto di ciascun Contratto esecutivo per la verifica della corretta esecuzione delle prestazioni contrattuali; tale verifica, che potrà essere eseguita anche a campione, verrà effettuata, su richiesta di ciascuna Amministrazione secondo le modalità e le specifiche stabilite nell'Accordo Quadro e nel Capitolato Tecnico Generale e Speciale.

La verifica di conformità sarà svolta dalle Amministrazioni nel rispetto di quanto stabilito dagli artt. 101 e 102 del D. Lgs. n. 50/2016, nonché di quanto previsto nei provvedimenti di attuazione.
2. Le verifiche di conformità di cui ai precedenti commi si intendono positivamente superate solo se le verifiche abbiano dato esito positivo ed i servizi siano risultati conformi alle prescrizioni dell'Accordo Quadro, del Capitolato Tecnico Generale e Speciale e dell'offerta tecnica, ove migliorativa; tutti gli oneri e le spese delle verifiche di conformità sono a carico del Fornitore.
3. Nel caso di esito positivo della verifica di conformità relativamente ai servizi di compliance e controllo la data del relativo verbale verrà considerata quale "Data di accettazione".
4. Nel caso di esito negativo della verifica di conformità e/o di esito negativo delle verifiche di funzionalità effettuate in corso d'opera a norma del successivo comma, il Fornitore dovrà svolgere ogni attività necessaria affinché la verifica sia ripetuta e positivamente superata, salvo in ogni caso l'applicazione delle penali di cui oltre.
5. Conclusa positivamente la verifica di conformità, e comunque entro un termine non superiore a sette giorni dalla conclusione della stessa, l'Amministrazione Contraente rilascia il certificato di pagamento o altro documento equivalente ai fini dell'emissione della fattura da parte dell'appaltatore.
6. Le Amministrazioni Contraenti e la Consip S.p.A., per quanto di propria competenza, potranno effettuare unilaterali verifiche, anche in corso d'opera, per l'accertamento della conformità dei servizi resi disponibili.
7. Su richiesta del Fornitore, il Responsabile del Procedimento dell'Amministrazione contraente emetterà il certificato di esecuzione prestazioni dei servizi (CES), coerentemente al modello predisposto dall'Autorità Nazionale Anticorruzione. Il certificato verrà emesso solo a seguito della verifica, da parte dell'Amministrazione contraente, dell'avvenuta erogazione dei servizi oggetto del Contratto esecutivo e della conseguente verifica di conformità della

Classificazione del documento: Consip Public





fornitura predetta, nel rispetto delle prescrizioni contrattuali e della normativa vigente.

8. In caso di mancata attestazione di regolare esecuzione, la singola Amministrazione potrà risolvere il Contratto esecutivo e provvederà a dare comunicazione a Consip S.p.A. la quale potrà risolvere il presente Accordo Quadro.

#### **ARTICOLO 10 - CORRISPETTIVI E FATTURAZIONE**

1. I corrispettivi dovuti al Fornitore dalle singole Amministrazioni Contraenti per le prestazioni oggetto di ciascun Contratto esecutivo sono indicati nell'Offerta Economica, di cui all'Allegato **"B"** del presente Accordo Quadro e nel documento riepilogativo allegato sub **"C"** (Corrispettivi e tariffe PAL).
2. I corrispettivi, indicati nell'Accordo Quadro, si riferiscono ai servizi prestati a perfetta regola d'arte e nel pieno adempimento delle modalità e delle prescrizioni contrattuali.
3. Tutti gli obblighi ed oneri derivanti al Fornitore dall'esecuzione dell'Accordo Quadro e dei singoli Contratti esecutivi, dall'osservanza di leggi e regolamenti, nonché dalle disposizioni emanate o che venissero emanate dalle competenti Autorità, sono compresi nel corrispettivo contrattuale.
4. I corrispettivi contrattuali sono stati determinati a proprio rischio dal Fornitore in base ai propri calcoli, alle proprie indagini, alle proprie stime, e sono, pertanto, fissi ed invariabili indipendentemente da qualsiasi imprevisto o eventualità, facendosi carico il Fornitore medesimo di ogni relativo rischio e/o alea. Il Fornitore non potrà vantare diritto ad altri compensi, ovvero ad adeguamenti, revisioni o aumenti dei corrispettivi come sopra indicati.
5. Tali corrispettivi sono dovuti dalle Amministrazioni Contraenti al Fornitore a decorrere dalla "Data di accettazione", successivamente all'esito positivo della verifica di conformità della prestazione.
6. Ciascuna fattura dovrà contenere, oltre alle indicazioni che verranno fornite dall'Amministrazione, il riferimento all'Accordo Quadro, al singolo Contratto esecutivo, cui si riferisce e dovrà essere intestata e trasmessa alla Amministrazione. Il CIG (Codice Identificativo Gara) "derivato" rispetto a quello dell'Accordo Quadro o il CUP (Codice Unico di Progetto) ove obbligatorio ai sensi dell'art. 11 della Legge 16 gennaio 2003, comunicato dalle Amministrazioni sarà inserito, a cura del Fornitore, nelle fatture e dovrà essere indicato dalle Amministrazioni nei rispettivi pagamenti ai fini dell'ottemperanza agli obblighi scaturenti dalla normativa in tema di tracciabilità dei flussi finanziari.
7. Nel caso in cui l'aggiudicatario sia un R.T.I., gli obblighi di cui sopra dovranno essere tutti puntualmente assolti sia nelle fatture emesse dalla mandataria, sia dalle mandanti, nel rispetto delle condizioni e delle modalità tutte disciplinate dai successivi comma del presente articolo.
8. I predetti corrispettivi saranno fatturati con la cadenza indicata in sede di Contratto esecutivo e saranno corrisposti dalle Amministrazioni secondo la normativa vigente in materia di Contabilità delle Amministrazioni Contraenti e previo accertamento della prestazione effettuate.
9. Ciascuna fattura dovrà essere inviata in forma elettronica in osservanza delle modalità previste dal D. Lgs. 20 febbraio 2004 n. 52, dal D. Lgs. 7 marzo 2005 n. 82 e dai successivi decreti attuativi. Il Fornitore si impegna, inoltre, ad inserire nelle fatture elettroniche i dati e le informazioni che la singola Amministrazione Contraente riterrà di richiedere, nei limiti delle disposizioni normative vigenti.
10. Ai fini del pagamento di corrispettivi di importo superiore ad euro 5.000,00, l'Amministrazione Contraente procederà in ottemperanza alle disposizioni previste dall'art. 48-bis del D.P.R. 602 del 29 settembre 1973, con le modalità di cui al Decreto del Ministero dell'Economia e delle Finanze del 18 gennaio 2008 n. 40.
11. Rimane inteso che l'Amministrazione prima di procedere al pagamento del corrispettivo acquisirà di ufficio il documento unico di regolarità contributiva (D.U.R.C.) - attestante la regolarità del Fornitore in ordine al versamento dei contributi previdenziali e dei contributi assicurativi obbligatori per gli infortuni sul lavoro e le malattie professionali dei dipendenti.

Classificazione del documento: Consip Public

Accordo Quadro avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni - ID SIGEF 2296

Accordo Quadro Lotto 2



12. A decorrere dal 1 Febbraio 2020, per gli acquisti di beni, e dal 1 Gennaio 2021, per gli acquisti di servizi, ai sensi dell'articolo 1, comma 412, della legge 31 dicembre 2009, n. 196 nonché dall'articolo 3 del Decreto del Ministro dell'Economia e delle Finanze 7 dicembre 2018, così come modificato dal Decreto del Ministero dell'Economia e delle Finanze 27 dicembre 2019, e in conformità alle "Linee Guida per l'emissione della trasmissione degli ordini elettronici adottate dal Ministero dell'Economia e delle Finanze" in data 29 dicembre 2020, l'Amministrazione Contraente rientrando nell'ambito applicativo della normativa sopra richiamata, dovrà, fatta eccezione per le esclusioni previste dal par. 3.1.2 delle richiamate Linee guida, trasmettere al Nodo di Smistamento degli Ordini di acquisto (NSO), il documento informatico attestante l'Ordinativo di Fornitura stesso (di seguito "Ordine NSO"). A tal fine, l'Amministrazione Contraente utilizza la funzione di trasmissione automatica al NSO, disponibile sul Sistema di e-procurement di Consip S.p.A., o, in alternativa, trasmette, l'Ordine NSO attraverso altre piattaforme.
13. Ciascuna fattura relativa agli acquisti, da e per conto degli enti del Servizio sanitario nazionale, di cui all'articolo 19, comma 2, lettere b) e c), del D. Lgs. 23 giugno 2011, n. 118, dovrà riportare gli estremi dei documenti informatici attestanti l'ordinazione e l'esecuzione dell'acquisto, trasmessi per mezzo del NSO. Qualora la fattura non indichi gli estremi dell'Ordine NSO da cui promana, a causa del mancato invio dell'Ordine NSO da parte dell'Ente, quest'ultimo è tenuto a provvedere al mancato invio con la trasmissione di un Ordine di convalida, secondo le modalità indicate nelle Linee Guida sopra richiamate.
14. Le Amministrazioni contraenti opereranno sull'importo netto progressivo delle prestazioni una ritenuta dello 0,5 % che verrà liquidata dalle stesse solo al termine del Contratto esecutivo; le ritenute possono essere svincolare solo in sede di liquidazione finale, in seguito all'approvazione del certificato di verifica di conformità e previa acquisizione del documento unico di regolarità contributiva.
15. I termini di pagamento delle predette fatture saranno definiti secondo le modalità di cui alla normativa vigente, e, in particolare, dell'art. 113 bis del Codice e del D.Lgs. n. 231/2002 s.m.i. I corrispettivi saranno accreditati, a spese dell'Amministrazione Contraente o del Fornitore ove sia previsto da norme di legge o regolamentari, sul conto corrente:
  - n. 000002249262, intestato al Fornitore Deloitte Risk Advisory S.r.l. S.B. presso Monte dei Paschi di Siena, Codice IBAN IT62G0103001654000002249262;
  - n. 000000000240, intestato al Fornitore Deloitte Risk Advisory S.r.l. S.B. presso Barclays Bank Plc., Codice IBAN IT18K0305101699000000000240;
  - n. 000052032893, intestato al Fornitore Deloitte Risk Advisory S.r.l. S.B. presso Ing Bank NV., Codice IBAN IT96V0347501601000052032893;
  - n. 000042210925, intestato al Fornitore Deloitte Risk Advisory S.r.l. S.B. presso BPER Banca S.p.A., Codice IBAN IT69K0538701615000042210925;
  - n. 000000023679, intestato al Fornitore Deloitte Risk Advisory S.r.l. S.B. presso Banco BPM S.p.A., Codice IBAN IT20F0503401727000000023679;
  - n. 000008195207, intestato al Fornitore Deloitte Risk Advisory S.r.l. S.B. presso Banca Intesa SanPaolo, Codice IBAN IT17X0306909400000008195207;
  - n. 00045200806, intestato al Fornitore Deloitte Risk Advisory S.r.l. S.B. presso Cariparma Crédit Agricole, Codice IBAN IT46T0623001627000045200806;
  - n. 000000201088, intestato al Fornitore Deloitte Risk Advisory S.r.l. S.B. presso Banca di Credito Cooperativo di Carate Brianza, Codice IBAN IT92O0844001601000000201088;
  - n. 000000000004, intestato al Fornitore Deloitte Risk Advisory S.r.l. S.B. presso Banca Nazionale del Lavoro, Codice IBAN IT76H0100501600000000000004;
  - n. CC0100061376, intestato al Fornitore Deloitte Risk Advisory S.r.l. S.B. presso Banca FINNAT, Codice

Classificazione del documento: Consip Public

Accordo Quadro avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni - ID SIGEF 2296

Accordo Quadro Lotto 2



IBAN IT22F0308703200CC0100061376;

- n. 000042205764, intestato al Fornitore EY Advisory S.p.A. presso BPER BANCA S.p.A – Filiale 01615 - Via della Moscova 31/A Milano, Codice IBAN IT92C0538701615000042205764;
- n. 000070473242, intestato al Fornitore Teleco S.r.l. presso Banco di Sardegna S.p.A – Filiale di Cagliari Agenzia 1 – Viale Trieste Cagliari, Codice IBAN IT13N0101504801000070473242;

Il Fornitore dichiara che il predetto conto opera nel rispetto della Legge 13 agosto 2010 n. 136 e s.m.i.

16. Il Fornitore si obbliga a comunicare le generalità e il codice fiscale del/i delegato/i ad operare sul/i predetto/i conto/i alle Amministrazioni all'atto dell'accettazione del Piano dei Fabbisogni secondo le modalità indicate all'art.6.
17. In caso di ritardo nei pagamenti, il tasso di mora viene stabilito in una misura pari al tasso BCE stabilito semestralmente e pubblicato con comunicazione del Ministero dell'Economia e delle Finanze sulla G.U.R.I., maggiorato di 8 punti, secondo quanto previsto nell'art. 5 del D.Lgs. 9 ottobre 2002, n. 231.
18. Il Fornitore, sotto la propria esclusiva responsabilità, renderà tempestivamente noto alle Amministrazioni e alla Consip S.p.A., per quanto di propria competenza, le variazioni che si verificassero circa le modalità di accredito indicate nell'Accordo Quadro e nei singoli Contratti esecutivi; in difetto di tale comunicazione, anche se le variazioni venissero pubblicate nei modi di legge, il Fornitore non potrà sollevare eccezioni in ordine ad eventuali ritardi dei pagamenti, né in ordine ai pagamenti già effettuati.
19. Nel caso in cui risulti aggiudicatario dell'Accordo Quadro un R.T.I., le singole imprese costituenti il Raggruppamento, salva ed impregiudicata la responsabilità solidale delle società raggruppate nei confronti dell'Amministrazione Contraente, dovranno provvedere ciascuna alla fatturazione delle sole attività effettivamente svolte, corrispondenti alle attività dichiarate in fase di gara risultanti nell'atto costitutivo del Raggruppamento Temporaneo di Imprese, che il Fornitore si impegna a trasmettere in copia, ove espressamente richiesto dall'Amministrazione Contraente. Ogni singola fattura dovrà contenere la descrizione di ciascuno dei servizi e/o forniture cui si riferisce.
20. Il R.T.I. avrà facoltà di scegliere se: i) il pagamento da parte delle Amministrazioni Contraenti dovrà essere effettuato nei confronti della mandataria che provvederà poi alla redistribuzione dei corrispettivi a favore di ciascuna mandante in ragione di quanto di spettanza o ii) se, in alternativa, il pagamento dovrà essere effettuato dalle Amministrazioni Contraenti direttamente a favore di ciascun membro del RTI. La predetta scelta dovrà risultare dall'atto costitutivo del RTI medesimo. In ogni caso, la società mandataria del Raggruppamento medesimo è obbligata a trasmettere apposito prospetto riepilogativo delle attività e delle competenze maturate dalle singole imprese membri del RTI e, in maniera unitaria, le fatture di tutte le imprese raggruppate e prospetto riepilogativo delle attività e delle competenze maturate da ciascuna. Resta in ogni caso fermo quanto previsto dall'art. 48, comma 13, del D.Lgs. n. 50/2016.
21. Resta tuttavia espressamente inteso che in nessun caso il Fornitore potrà sospendere la prestazione dei servizi e, comunque, delle attività previste nell'Accordo Quadro e nei singoli Contratti esecutivi, salvo quanto diversamente previsto nell'Accordo Quadro medesimo.
22. Qualora il Fornitore si rendesse inadempiente a tale obbligo, i singoli Contratti esecutivi e/o l'Accordo Quadro si potranno risolvere di diritto mediante semplice ed unilaterale dichiarazione da comunicarsi tramite pec o con lettera raccomandata A/R, rispettivamente dalle Amministrazioni Contraenti e dalla Consip S.p.A., ciascuno per quanto di propria competenza.
23. E' ammessa la cessione dei crediti maturati dal Fornitore nei confronti dell'Amministrazione a seguito della regolare e corretta esecuzione delle prestazioni oggetto del Contratto esecutivo, nel rispetto dell'art. 106, comma 13, del D.Lgs. n. 50/2016. In ogni caso, è fatta salva ed impregiudicata la possibilità per l'Amministrazione Contraente di opporre al cessionario tutte le medesime eccezioni opponibili al Fornitore cedente. Le cessioni dei crediti devono essere stipulati mediante atto pubblico o scrittura privata autenticata e devono essere notificate alla

Classificazione del documento: Consip Public

Accordo Quadro avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni - ID SIGEF 2296

Accordo Quadro Lotto 2



Amministrazione Contraente. Si applicano le disposizioni di cui alla Legge n. 52/1991. Resta fermo quanto previsto in tema di tracciabilità dei flussi finanziari di cui al successivo articolo 25.

24. Ai fini del versamento dell'IVA per cessione di beni e prestazioni di servizi a favore delle Pubbliche Amministrazioni, si applica quanto previsto dall'art. 17-ter del d.P.R. n. 633 del 1972 ("split payment"), introdotto dall'art. 1, comma 629, della legge n. 190 del 2014, come modificato dal D.L. 24 aprile 2017, n. 50, convertito dalla legge 21 giugno 2017, n. 96, e le relative disposizioni di attuazione tra le quali il DM 23 gennaio 2015 come modificato dal DM 27 giugno 2017.
25. In caso di pericolo di insolvenza di Organismi di diritto pubblico, di cui all'art. 3 comma 1, lett. d), del D.Lgs. n. 50/2016, diversi dalle società pubbliche inserite nel conto economico consolidato della pubblica amministrazione, come individuate dall'Istituto nazionale di statistica (ISTAT) ai sensi dell'articolo 1 della legge 31 dicembre 2009, n. 196, a totale partecipazione pubblica diretta o indiretta, è facoltà del Fornitore non inadempiente richiedere di prestare idonea garanzia per l'adempimento dell'obbligazione di pagamento relativa al contratto esecutivo; tale garanzia dovrà essere rilasciata per un importo pari al 20% del valore del Contratto esecutivo. La garanzia dovrà essere richiesta dal Fornitore entro il termine di 4 giorni lavorativi dalla ricezione dell'ordine e l'Amministrazione dovrà rilasciarla entro 30 giorni dalla ricezione della richiesta. Il Fornitore non inadempiente è legittimato a sospendere l'esecuzione della fornitura fino ad avvenuta ricezione della garanzia richiesta. Decorso inutilmente il termine per il rilascio della garanzia e ferma restando la facoltà di sospensione dell'esecuzione, è facoltà del Fornitore, ai sensi dell'art. 1454 c.c., diffidare per iscritto l'Amministrazione ad adempiere entro 15 giorni, decorsi inutilmente i quali il contratto s'intenderà risolto di diritto. Resta salva la facoltà dell'Amministrazione di recedere dal contratto esecutivo in caso di sospensione.
26. In caso di Contratti esecutivi effettuati da Organismi di diritto pubblico, di cui all'art. 3 comma 1, lett. d), del D.Lgs. n. 50/2016, verso i quali il Fornitore vanta un credito certo, liquido, esigibile e non più contestabile, maturato del presente AQ o in precedenti rapporti contrattuali, il Fornitore è legittimato a sospendere l'esecuzione del Contratto esecutivo fino ad avvenuta ricezione della comprova del pagamento per l'adempimento del debito pregresso. A tal fine il Fornitore dovrà fornire adeguata documentazione del credito vantato, ivi inclusa la specificazione delle fatture non pagate. Resta salva la facoltà dei suddetti soggetti di recedere dal contratto esecutivo in caso di sospensione.
27. Fermo restando quanto stabilito al precedente comma, in caso di Contratti esecutivi effettuati da Amministrazioni verso le quali il Fornitore vanta un credito certo, liquido, esigibile e non più contestabile, maturato nel presente Accordo Quadro ovvero in precedenti rapporti contrattuali relativi alla fornitura di beni o servizi ricompresi nell'oggetto dell'Accordo Quadro, il Fornitore è legittimato a sospendere l'esecuzione del contratto esecutivo fino ad avvenuta ricezione della comprova del pagamento/stanziamiento di fondi per l'adempimento del debito pregresso. A tal fine il Fornitore dovrà fornire adeguata documentazione all'Amministrazione del credito vantato, ivi inclusa la specificazione delle fatture non pagate. Resta salva la facoltà dell'Amministrazione di recedere dal contratto esecutivo in caso di sospensione.
28. Gli Organismi di diritto pubblico, di cui all'art. 3 comma 1, lett. d), del D.Lgs. n. 50/2016, nel Contratto esecutivo, accettano preventivamente la cessione dei crediti ai sensi e per gli effetti di cui all'art. 106, comma 13 del D.Lgs. n. 50/2016.
29. Ove applicabile in considerazione della natura e tipologia di prestazioni, ai sensi dell'art. 35, comma 18, del Codice, così come novellato dal D.L. 32/2019, il fornitore può ricevere, entro 15 giorni dall'effettivo inizio delle prestazioni oggetto del Contratto esecutivo un'anticipazione del prezzo pari al 20 per cento del valore del Contratto esecutivo stesso. Tale percentuale può essere aumentata dall'Amministrazione Contraente fino ad un massimo del 30% al ricorrere dei presupposti di cui all'art. 207 del D.L. 34/2020.

Classificazione del documento: Consip Public

Accordo Quadro avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni - ID SIGEF 2296

Accordo Quadro Lotto 2



L'erogazione dell'anticipazione è subordinata alla costituzione di una garanzia fideiussoria bancaria o assicurativa in favore dell'Amministrazione beneficiaria della prestazione, rilasciata dai soggetti indicati all'art. 35, comma 18, del Codice, di importo pari all'anticipazione, maggiorato del tasso di interesse legale applicato al periodo necessario al recupero dell'anticipazione stessa secondo il cronoprogramma (o altro documento equivalente tipo SLA) della prestazione che sarà indicato nel Piano dei Fabbisogni.

30. L'importo della garanzia viene gradualmente ed automaticamente ridotto nel corso dello svolgimento delle prestazioni, in rapporto al progressivo recupero dell'anticipazione da parte delle Amministrazioni.
31. Il Fornitore decade dall'anticipazione, con obbligo di restituzione delle somme anticipate, se l'esecuzione delle prestazioni, non procede, per ritardi a lui imputabili, secondo il cronoprogramma concordato. Sulle somme restituite sono dovuti gli interessi legali con decorrenza dalla data di erogazione della anticipazione.
32. Laddove in relazione al singolo contratto esecutivo ricorrano i presupposti soggettivi ed oggettivi, le Amministrazioni Contraenti e il Fornitore sono tenuti all'applicazione delle disposizioni di cui all'art. 17-bis del D.lgs. 241/1997 in materia di ritenute e compensazioni in appalti e subappalti.

#### **ARTICOLO 11 - COSTI DELLA SICUREZZA**

1. Stante la natura delle prestazioni oggetto di Accordo Quadro non è prevista la redazione del "Documento di valutazione dei rischi standard da interferenze".

#### **ARTICOLO 12 - PENALI**

1. Si applicano le penali previste nell'appendice 1 al Capitolato Tecnico Speciale (che deve intendersi in questa sede integralmente trascritta), nonché quelle di seguito indicate. È sempre fatto salvo il risarcimento del maggior danno. In caso di penali da ritardo, deve considerarsi ritardo anche il caso in cui il Fornitore esegua il servizio in modo anche solo parzialmente difforme rispetto alle disposizioni di cui al presente Accordo Quadro, al Capitolato Tecnico Generale, al Capitolato Tecnico Speciale e al singolo Contratto esecutivo, nonché alla propria Offerta Tecnica. In tal caso le Amministrazioni applicheranno al Fornitore la suddetta penale sino alla data in cui il servizio inizierà ad essere eseguito in modo effettivamente conforme al presente Accordo Quadro, al Capitolato Tecnico Generale, al Capitolato Tecnico Speciale e al singolo Contratto esecutivo, all'Offerta Tecnica, fatto salvo il risarcimento del maggior danno.
2. In caso di invio della documentazione necessaria all'attivazione dell'Accordo Quadro (ivi compreso il Piano di Qualità Generale) in ritardo rispetto ai termini previsti nel presente Accordo Quadro e relativi allegati o di ritardo nell'attivazione del portale della fornitura, per cause non imputabili a Consip ovvero a forza maggiore o caso fortuito, Consip avrà la facoltà di applicare una penale pari a 1.000,00 euro per ogni giorno solare di ritardo, fatto salvo il risarcimento del maggior danno subito.
3. In caso di invio della documentazione prodromica alla stipula di ciascun Contratto Esecutivo (ivi compreso il Piano Operativo e relativi allegati e i riferimenti del RUAC del Contratto Esecutivo) in ritardo rispetto ai termini previsti nel presente Accordo Quadro e relativi allegati o comunque concordati con l'Amministrazione, per cause non imputabili a Consip, all'Amministrazione ovvero a forza maggiore o caso fortuito, Consip, anche su segnalazione dell'Amministrazione, avrà la facoltà di applicare una penale pari a 1.000,00 euro per ogni giorno solare di ritardo, fatto salvo il risarcimento del maggior danno subito.
4. Per ogni giorno di ritardo del Fornitore, non imputabile a Consip S.p.A. ovvero a forza maggiore o caso fortuito, nell'adempimento all'obbligo previsto al precedente articolo 8, comma 1, lettere a), b) e c) per la presentazione della documentazione ivi indicata, il Fornitore è tenuto a corrispondere a Consip S.p.A. una penale pari a euro 100,00 = (cento/00), fatto salvo il risarcimento del maggior danno.

Classificazione del documento: Consip Public



5. Per ogni giorno di ritardo non imputabile all'Amministrazione, ovvero a forza maggiore o caso fortuito, i) rispetto ai previsti tempi di effettuazione delle verifiche di conformità; ii) di ripetizione delle prove di collaudo in caso di esito negativo delle verifiche di conformità; l'Amministrazione potrà applicare al Fornitore una penale pari allo 0,3 (ovvero in caso di Contratti esecutivi cd. PNRR o PNC si intenderà 0,6) per mille del valore del Contratto esecutivo, fatto salvo il risarcimento del maggior danno.
6. Nel caso in cui, come previsto nell'atto di nomina a responsabile del Trattamento allegato all'Accordo Quadro, all'esito delle verifiche, ispezioni e audit e assessment compiuti dall'Amministrazione o da terzi autorizzati, le misure di sicurezza adottate dal Responsabile primario/Sub responsabile/Terzo autorizzato al trattamento dovessero risultare inadeguate rispetto al rischio del trattamento o, comunque, inadeguate ad assicurare l'applicazione delle "*Norme in materia di protezione dei dati personali*", l'Amministrazione applicherà al Fornitore - Responsabile primario/Sub responsabile/Terzo autorizzato del trattamento una penale pari all' **1 per mille** del corrispettivo del singolo Contratto esecutivo per ogni giorno necessario per il Fornitore per l'adozione di misure di sicurezza idonee ad assicurare l'applicazione delle "*Norme in materia di protezione dei dati personali*", salvo il maggior danno.
7. Gli eventuali inadempimenti contrattuali che daranno luogo all'applicazione delle penali sopra stabilite, dovranno essere contestati al Fornitore per iscritto da Consip S.p.A. e/o dalla singola Amministrazione, per quanto di rispettiva competenza; in quest'ultimo caso, gli eventuali inadempimenti dovranno essere comunicati dalle Amministrazioni per conoscenza a Consip S.p.A.
8. In caso di mancato adempimento anche ad una sola delle obbligazioni di cui al precedente art. 7, comma 15 il Fornitore sarà tenuto a corrispondere, ai sensi dell'art. 47, comma 6 della L. n. 108/2021 una penale pari a euro 25.000,00. Il mancato adempimento dell'invio della documentazione richiesta entro 30 giorni dall'applicazione della penale comporta l'applicazione di una ulteriore penale del medesimo importo fino ad avvenuto adempimento e comunque, a parziale deroga di quanto previsto dal successivo comma 13, per un importo complessivo non superiore al 20% del valore dell'Accordo Quadro. Si applica la delibera ANAC n. 122 del 16 marzo 2022 per la parte relativa alle Comunicazioni da inserire casellario informatico.
9. Per ogni punto percentuale di scostamento in diminuzione (arrotondato al numero intero) tra il valore percentuale misurato e il valore minimo richiesto al par. 7.1 del Capitolato Tecnico Generale (**dati per Consip**) Consip, si riserva di applicare una penale pari a euro 1.000,00.
10. Per ogni punto percentuale di scostamento in diminuzione (arrotondato al numero intero) tra il valore percentuale minimo richiesto al par. 7.1 del Capitolato Tecnico Generale (**dati per Amministrazione**) e il valore percentuale come eventualmente migliorato nella propria offerta tecnica dal Fornitore l'Amministrazione, si riserva di applicare una penale pari a euro 1.000,00.
11. In caso di contestazione dell'inadempimento da parte di Consip S.p.A. e/o della singola Amministrazione, per quanto di rispettiva competenza, il Fornitore dovrà comunicare, in ogni caso, per iscritto, le proprie deduzioni, supportate da una chiara ed esauriente documentazione, nel termine massimo di n. 5 (cinque) giorni lavorativi dalla ricezione della contestazione stessa. Qualora le predette deduzioni non pervengano a Consip S.p.A. e/o all'Amministrazione nel termine indicato, ovvero, pur essendo pervenute tempestivamente, non siano idonee, a giudizio di Consip S.p.A. e/o dall'Amministrazione, a giustificare l'inadempimento, potranno essere applicate al Fornitore le penali stabilite nell'Accordo Quadro a decorrere dall'inizio dell'inadempimento.
12. Consip S.p.A. potrà per l'applicazione delle penali dell'Accordo Quadro avvalersi della garanzia disciplinata nell'Accordo Quadro, senza bisogno di diffida, ulteriore accertamento o procedimento giudiziario. Le singole Amministrazioni potranno compensare i crediti derivanti dall'applicazione delle penali di cui all'Accordo Quadro con quanto dovuto al Fornitore a qualsiasi titolo, quindi anche con i corrispettivi maturati, ovvero avvalersi della garanzia disciplinata nell'Accordo Quadro, senza bisogno di diffida, ulteriore accertamento o procedimento giudiziario.

Classificazione del documento: Consip Public

Accordo Quadro avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni - ID SIGEF 2296

Accordo Quadro Lotto 2





13. Consip S.p.A., per le parti di sua competenza, potrà applicare al Fornitore penali sino a concorrenza della misura massima pari al 10% (dieci per cento) del valore dell'Accordo Quadro, fermo il risarcimento degli eventuali maggiori danni, nonché la risoluzione contrattuale per inadempimenti che comportino l'applicazione di penali oltre la predetta misura massima.
14. Le Amministrazioni, per le parti di loro competenza, potranno applicare al Fornitore penali sino a concorrenza della misura massima:
- pari al 20% (venti per cento), per i contratti finanziati in tutto o in parte con i fondi del PNRR e del PNC,
  - ovvero
  - pari al 10% (dieci per cento), per i contratti non finanziati con i fondi del PNRR o del PNC;
- del Contratto di Fornitura, fermo il risarcimento degli eventuali maggiori danni, nonché la risoluzione contrattuale per inadempimenti che comportino l'applicazione di penali oltre la predetta misura massima.
15. La richiesta e/o il pagamento delle penali non esonera in nessun caso il Fornitore dall'adempimento dell'obbligazione per la quale si è reso inadempiente e che ha fatto sorgere l'obbligo di pagamento della medesima penale.

### **ARTICOLO 13 - GARANZIE**

1. A garanzia delle obbligazioni contrattuali assunte nei confronti della Consip S.p.A. dal Fornitore con la stipula della Accordo Quadro, il Fornitore medesimo ha prestato garanzia definitiva rilasciata in data 31/01/2022 dalla Euler Hermes avente n. 2565421 di importo pari ad Euro 400.000,00 = (quattrocentomila/00).
2. In particolare, la garanzia rilasciata garantisce tutti gli obblighi specifici assunti dal Fornitore, anche quelli a fronte dei quali è prevista l'applicazione di penali da parte di Consip e quelli derivanti dal rispetto del patto di integrità, pertanto, resta espressamente inteso che la stessa Consip, fermo restando quanto previsto nel precedente articolo 12, ha diritto di rivalersi direttamente sulla garanzia per l'applicazione delle penali. Tale garanzia copre altresì la serietà dell'offerta dell'aggiudicatario nell'ambito della fase di affidamento dei singoli Contratti esecutivi prevista dal paragrafo 6.5 del Capitolato Tecnico Generale e dall'art. 6 del presente documento, ivi compresa la fase di rilascio del Piano Operativo. La stessa garanzia verrà, altresì, escussa nel caso di dichiarazioni mendaci rese nell'ambito dell'aggiornamento della documentazione amministrativa di cui all'art. 8 dell'Accordo Quadro. In tal caso la Consip procederà, oltre alla risoluzione dell'Accordo Quadro, anche alla segnalazione del fatto all'Autorità Nazionale Anticorruzione.
3. La garanzia prestata in favore della Consip S.p.A. opera a far data dalla sottoscrizione dell'Accordo Quadro e per tutta la durata dell'Accordo Quadro e dei Contratti esecutivi, e, comunque, sino alla completa ed esatta esecuzione delle obbligazioni nascenti dai predetti contratti.
4. A garanzia delle obbligazioni contrattuali assunte dal Fornitore con la stipula dell'Accordo Quadro e dei relativi Contratti esecutivi, il Fornitore medesimo si è impegnato a prestare in favore di ciascuna Amministrazione Contraente la relativa garanzia definitiva in conformità al modello 2 di cui all'Allegato 14 della documentazione di gara.
5. La garanzia copre tutti gli obblighi specifici assunti dal Fornitore con i contratti esecutivi nei confronti delle Amministrazioni, anche quelli a fronte dei quali è prevista l'applicazione di penali da parte delle stesse e, pertanto, resta espressamente inteso che le Amministrazioni hanno diritto di rivalersi direttamente sulla garanzia per l'applicazione delle penali. La garanzia copre altresì il risarcimento dei danni derivanti dall'eventuale inadempimento delle obbligazioni stesse, nonché il rimborso delle somme pagate in più all'esecutore rispetto alle risultanze della liquidazione finale, salva comunque la risarcibilità del maggior danno verso l'appaltatore, nonché il rispetto degli impegni assunti con il Patto di integrità, l'eventuale maggiore spesa sostenuta per il completamento delle prestazioni nel caso di risoluzione dei contratti esecutivi disposta in danno dell'esecutore, il pagamento di quanto dovuto dall'esecutore per le inadempienze derivanti dalla

Classificazione del documento: Consip Public



- inosservanza di norme e prescrizioni dei contratti collettivi, delle leggi e dei regolamenti sulla tutela, protezione, assicurazione, assistenza e sicurezza fisica dei lavoratori.
6. La garanzia prestata in favore delle Amministrazioni decorre dalla data di stipula di ciascun contratto esecutivo e cessa alla data di emissione del certificato di verifica di conformità o dell'attestazione di regolare esecuzione delle prestazioni, emessi alla conclusione dell'esecuzione del medesimo contratto e comunque decorsi 12 mesi dalla data di ultimazione delle prestazioni contrattuali risultante dal relativo certificato dell'ultimo contratto esecutivo, allorché si estingue automaticamente ad ogni effetto (art. 103, commi 1 e 5, del Codice). Resta fermo quanto previsto nello schema tipo del DM 31/2018 come derogato dal Capitolato d'Oneri.
  7. Le garanzie di cui ai precedenti commi prevedono espressamente la rinuncia al beneficio della preventiva escussione del debitore principale, la rinuncia all'eccezione di cui all'articolo 1957, comma 2, del codice civile, nonché l'operatività della garanzia medesima – anche per il recupero delle penali contrattuali - entro quindici giorni, a semplice richiesta scritta del rispettivo beneficiario.
  8. E' onere della singola Amministrazione comunicare alla Consip S.p.a. l'importo delle somme percepite dal Garante.
  9. Le garanzie di cui ai commi precedenti sono progressivamente svincolate in ragione e a misura dell'avanzamento dell'esecuzione, nel limite massimo dell'80 per cento dell'iniziale importo garantito secondo quanto stabilito all'art. 103, comma 5, del D.Lgs. n. 50/2016. Lo svincolo avviene subordinatamente alla preventiva consegna al Garante ed alla Consip S.p.A da parte del Fornitore, in relazione ai contratti stipulati nell'arco temporale di riferimento, di: (i) documenti delle Amministrazioni, in originale o in copia autentica, attestanti la corretta esecuzione delle prestazioni, ai sensi dell'articolo 102 del D.Lgs. n. 50/2016; e/o (ii) documentazione comprovante l'avvenuta ricezione del rimborso della ritenuta di legge dello 0,5%, di cui al precedente articolo 10, comma 14. Il Garante dovrà comunicare alla Consip il valore dello svincolo. La Consip S.p.a. si riserva di verificare la correttezza degli importi svincolati e di chiedere al Fornitore ed al Garante in caso di errore un'integrazione.
  10. In alternativa a quanto sopra, il Fornitore potrà consegnare alla Consip S.p.a. un prospetto contenente l'elenco delle Amministrazioni Contraenti con l'ammontare delle fatture emesse nel relativo arco temporale e regolarmente saldate, unitamente al dettaglio specifico della posizione di ciascuna singola Amministrazione Contraente (numero fattura, numero contratto, mensilità di riferimento, data emissione, data pagamento, importo corrisposto), accompagnato da dichiarazione resa dal legale rappresentante del Fornitore o procuratore speciale munito dei necessari poteri, ai sensi del D.P.R. n. 445/2000, attestante la veridicità di tutte le informazioni contenute nel prospetto stesso e l'assenza di ogni contestazione sulle prestazioni eseguite e in esso consuntivate. La Consip S.p.a. procederà ad autorizzare lo svincolo comunicandolo al Garante e al Fornitore.
  11. Ai fini dello svincolo dell'ammontare residuo delle garanzie (20%), il Fornitore dovrà produrre, in relazione ai rimanenti Contratti esecutivi: (i) i certificati di verifica di conformità o le attestazioni di regolare esecuzione delle prestazioni emessi alla conclusione dell'esecuzione dei contratti esecutivi; e/o (ii) documentazione comprovante il rimborso della ritenuta di legge dello 0,5%, di cui al precedente articolo 10, comma 14.
  12. Qualora l'ammontare delle garanzie prestate dovesse ridursi per effetto dell'applicazione di penali, o per qualsiasi altra causa, il Fornitore dovrà provvedere al reintegro entro il termine di 10 (dieci) giorni lavorativi dal ricevimento della relativa richiesta effettuata dalla Consip S.p.A., pena la risoluzione della Accordo Quadro e/o dei singoli contratti esecutivi.
  13. In caso di inadempimento alle obbligazioni previste nel presente articolo la Consip S.p.A. ha facoltà di dichiarare risolto l'Accordo Quadro e, del pari, le singole Amministrazioni Contraenti hanno facoltà di dichiarare risolto il

Classificazione del documento: Consip Public





contratto esecutivo, fermo restando il risarcimento del danno.

14. In ogni caso il garante sarà liberato dalle garanzie prestate di cui ai commi precedenti solo previo consenso espresso in forma scritta dalla Consip S.p.A..

#### **ARTICOLO 14 - RISOLUZIONE**

1. Consip e/o le Amministrazioni, per quanto di rispettiva competenza, senza bisogno di assegnare alcun termine per l'adempimento, potranno risolvere l'Accordo Quadro e il singolo Contratto esecutivo ai sensi dell'art. 1456 cod. civ., nonché ai sensi dell'art.1360 cod. civ., previa dichiarazione da comunicarsi all'Impresa tramite pec, nei seguenti casi:
  - a) il Fornitore si è trovato, al momento dell'aggiudicazione dell'Accordo Quadro in una delle situazioni di cui all'articolo 80, comma 1, del d. lgs. n. 50/2016 e s.m.i. e avrebbe dovuto pertanto essere escluso dalla gara;
  - b) il Fornitore ha commesso, nella procedura di aggiudicazione del presente Accordo Quadro e/o dei successivi Contratti esecutivi, un illecito antitrust accertato con provvedimento esecutivo dell'AGCM, ai sensi dell'articolo 80, comma 5, lett. c) del d. lgs. n. 50/2016 e s.m.i. e secondo le linee guida A.N.AC.;
  - c) l'Accordo Quadro non avrebbe dovuto essere aggiudicato al Fornitore in considerazione di una grave violazione degli obblighi derivanti dai Trattati, come riconosciuto dalla Corte di giustizia dell'Unione europea in un procedimento ai sensi dell'articolo 258 TFUE;
  - d) qualora fosse accertata la non sussistenza ovvero il venir meno di uno dei requisiti minimi richiesti per la partecipazione alla gara, nonché per la stipula dell'Accordo Quadro e per lo svolgimento delle attività ivi previste;
  - e) qualora il Fornitore ponga in essere comportamenti tesi a eludere la modalità di affidamento dei Contratti esecutivi;
  - f) mancata copertura dei rischi durante tutta la vigenza dell'Accordo Quadro e dei Contratti esecutivi;
  - g) qualora il Fornitore, in esecuzione di un Contratto esecutivo, offra o fornisca la prestazione di servizi, che non abbiano i requisiti di conformità e/o le caratteristiche tecniche minime stabilite dalle normative vigenti, nonché nel Capitolato Tecnico Generale e Speciale, ovvero quelle migliorative eventualmente offerte in sede di aggiudicazione dell'Accordo Quadro;
  - h) mancata reintegrazione della garanzia di cui all'art. 13 eventualmente escussa entro il termine di 10 (dieci) giorni lavorativi dal ricevimento della relativa richiesta da parte della Consip S.p.A.;
  - i) azioni giudiziarie per violazioni di diritti di brevetto, di autore ed in genere di privativa altrui, intentate contro le Amministrazioni e/o la Consip S.p.A., ai sensi dell'articolo 21;
  - j) nei casi di cui agli articoli 9 (Verifiche di conformità); 10 (Corrispettivi e Fatturazione), 17 (Trasparenza), 18 (Riservatezza), 20 (Divieto di cessione del contratto), 24 (Codice Etico - Modello di organizzazione e gestione ex D.Lgs. n. 231/2001 - Piano Triennale per la prevenzione della corruzione e della trasparenza) e 25 (Tracciabilità dei flussi finanziari), 26 (Subappalto), 27 (Danni, responsabilità civile);
  - k) applicazione di penali oltre la misura massima stabilita all'articolo 12, commi 10 e 11;
  - l) nell'ipotesi di non veridicità delle dichiarazioni rese dal Fornitore ai sensi del D.p.r. n. 445/00, fatto salvo quanto previsto dall'art. 71, del medesimo D.P.R. 445/2000;
  - m) nell'ipotesi di irrogazione di sanzioni interdittive o misure cautelari di cui al D. Lgs. n. 231/01, che impediscano all'Impresa di contrattare con le Pubbliche Amministrazioni;
  - n) in caso di avalimento, ove a fronte delle segnalazioni delle Amministrazioni contraenti ed in ragione di quanto dichiarato dal Fornitore, risultasse la violazione dell'art. 89, comma 9, del d. lgs. n. 50/2016 e s.m.i.;
  - o) nei casi di cui all'articolo 3 e 5 del Patto di integrità.

Classificazione del documento: Consip Public



Nelle fattispecie di cui al presente comma non si applicano i termini previsti dall'articolo 21-nonies della legge 7 agosto 1990 n. 241.

2. Consip e/o le Amministrazioni Contraenti, per quanto di rispettiva competenza, devono risolvere l'Accordo Quadro e il singolo Contratto esecutivo senza bisogno di assegnare alcun termine per l'adempimento, ai sensi dell'art. 1456 cod. civ., nonché ai sensi dell'art. 1360 cod. civ., previa dichiarazione da comunicarsi all'Impresa tramite pec, nei seguenti casi:
  - a) qualora nei confronti del Fornitore sia intervenuto un provvedimento definitivo che dispone l'applicazione di una o più misure di prevenzione di cui al codice delle leggi antimafia e delle relative misure di prevenzione, fatto salvo quanto previsto dall'art. 95 del D. Lgs. n. 159/2011, o nel caso in cui gli accertamenti antimafia presso la Prefettura competente risultino positivi oppure sia intervenuta sentenza di condanna passata in giudicato per i reati di cui all'articolo 80 del D. Lgs. n. 50/2016 e s.m.i.;
  - b) qualora fosse accertato il venir meno dei requisiti-richiesti dalla legge;
3. Inoltre, Consip S.p.a. si impegna ad avvalersi della clausola risolutiva espressa di cui all'art. 1456 c.c. ogni qualvolta nei confronti del Fornitore o dei componenti la propria compagine sociale, o dei dirigenti dell'impresa con funzioni specifiche relative all'affidamento alla stipula e all'esecuzione dell'Accordo Quadro sia stata disposta misura cautelare o sia intervenuto rinvio a giudizio per taluno dei delitti di cui agli artt. 317 cp 318 cp 319 cp 319 bis cp 319 ter cp 319 quater 320 cp 322 cp 322 bis cp 346 bis cp 353 cp 353 bis cp. La risoluzione di cui al periodo precedente è subordinata alla preventiva comunicazione all'ANAC, cui spetta la valutazione in merito all'eventuale prosecuzione del rapporto contrattuale, al ricorrere delle condizioni di cui all'art. 32 del dl. 90/2014 convertito in legge 114 del 2014.
4. Il Fornitore accetta le cause di risoluzione previste nell'atto di nomina a Responsabile/sub Responsabile del Trattamento allegato al presente Accordo quadro, che devono intendersi integralmente trascritte.
5. Consip e/o le Amministrazioni Contraenti, quando accertino un grave inadempimento del Fornitore ad una delle obbligazioni assunte con l'Accordo Quadro e/o con i Contratti esecutivi tale da compromettere la buona riuscita delle prestazioni, formuleranno la contestazione degli addebiti al Fornitore e contestualmente assegneranno un termine, non inferiore a quindici giorni, entro i quali il Fornitore dovrà presentare le proprie controdeduzioni. Acquisite e valutate negativamente le controdeduzioni ovvero scaduto il termine senza che il Fornitore abbia risposto, Consip e/o le Amministrazioni Contraenti hanno la facoltà, per quanto di rispettiva competenza, di dichiarare la risoluzione di diritto dell'Accordo Quadro e/o dei Contratti esecutivi, di incamerare la garanzia ove essa non sia stata ancora restituita ovvero di applicare una penale equivalente, nonché di procedere all'esecuzione in danno dell'Impresa; resta salvo il diritto al risarcimento dell'eventuale maggior danno.
6. Qualora il Fornitore ritardi per negligenza l'esecuzione delle prestazioni rispetto alle previsioni dell'Accordo Quadro e dei Contratti esecutivi, Consip e/o le Amministrazioni contraenti assegnano un termine che, salvo i casi d'urgenza, non può essere inferiore a 10 (dieci) giorni, entro i quali il Fornitore deve eseguire le prestazioni. Scaduto il termine assegnato, e redatto processo verbale in contraddittorio con il Fornitore, qualora l'inadempimento permanga, Consip e/o le Amministrazioni contraenti potranno risolvere l'Accordo Quadro e/o i Contratti esecutivi, fermo restando il pagamento delle penali.
7. In caso di inadempimento del Fornitore anche a uno solo degli obblighi assunti con la stipula dell'Accordo Quadro e dei Contratti esecutivi che si protragga oltre il termine, non inferiore comunque a 15 (quindici) giorni, che verrà assegnato tramite pec dalla Consip e/o dall'Amministrazione Contraente, per quanto di propria competenza, per porre fine all'inadempimento, la Consip e/o l'Amministrazione Contraente hanno la facoltà di considerare risolti di diritto l'Accordo Quadro e/o i Contratti esecutivi e di ritenere definitivamente la

Classificazione del documento: Consip Public



garanzia ove essa non sia stata ancora restituita, e/o di applicare una penale equivalente, nonché di procedere nei confronti del Fornitore per il risarcimento del danno.

8. In caso di risoluzione anche di uno solo dei Contratti esecutivi, Consip S.p.A. si riserva di risolvere il presente Accordo Quadro. La risoluzione dell'Accordo Quadro legittima la risoluzione dei singoli Contratti esecutivi a partire dalla data in cui si verifica la risoluzione dell'Accordo Quadro. La risoluzione dell'Accordo Quadro è, pertanto, causa ostativa all'affidamento di nuovi Contratti esecutivi e può essere causa di risoluzione dei singoli Contratti esecutivi, salvo che non sia diversamente stabilito nei medesimi e salvo, in ogni caso, il risarcimento del danno.
9. In tutti i casi di risoluzione dell'Accordo Quadro e dei Contratti esecutivi, Consip S.p.A. e/o l'Amministrazione Contraente, avranno diritto di escutere la garanzia prestata per l'intero importo della stessa o per la parte percentualmente proporzionale all'importo del/i Contratto/i esecutivo/i risolto/i. Ove l'escussione non sia possibile sarà applicata una penale di equivalente importo, che sarà comunicata al Fornitore via pec. In ogni caso, resta fermo il diritto della medesima Amministrazione Contraente e/o di Consip S.p.A. al risarcimento dell'ulteriore maggior danno.
10. La Consip S.p.A., fermo restando quanto previsto nel presente articolo e nei casi di cui all'art. 110 del D.Lgs. n. 50/2016, potrà interpellare progressivamente gli operatori economici che hanno partecipato all'originaria procedura di gara e risultanti dalla relativa graduatoria al fine di stipulare un nuovo Accordo Quadro per l'affidamento del completamento delle prestazioni contrattuali alle medesime condizioni già proposte dall'aggiudicatario in sede di offerta.

#### **ARTICOLO 15 - RECESSO**

1. La Consip S.p.A. e/o le Amministrazioni, per quanto di proprio interesse, hanno diritto di recedere unilateralmente dal presente Accordo Quadro e/o da ciascun singolo Contratto esecutivo, in tutto o in parte, in qualsiasi momento, senza preavviso, nei casi di:
  - a) giusta causa,
  - b) reiterati inadempimenti del Fornitore, anche se non gravi.Si conviene che per giusta causa si intende, a titolo meramente esemplificativo e non esaustivo:
  - qualora sia stato depositato contro il Fornitore un ricorso ai sensi della legge fallimentare o di altra legge applicabile in materia di procedure concorsuali, che proponga lo scioglimento, la liquidazione, la composizione amichevole, la ristrutturazione dell'indebitamento o il concordato con i creditori, ovvero nel caso in cui venga designato un liquidatore, curatore, custode o soggetto avente simili funzioni, il quale entri in possesso dei beni o venga incaricato della gestione degli affari del Fornitore, resta salvo quanto previsto dall'art. 110, comma 3, del D.Lgs. n. 50/2016;
  - in qualsiasi altra fattispecie che faccia venire meno il rapporto di fiducia sottostante il presente Accordo Quadro o i Contratti esecutivi.
2. In caso di mutamenti di carattere organizzativo interessanti l'Amministrazione che abbiano incidenza sull'esecuzione della fornitura o della prestazione dei servizi, la stessa Amministrazione potrà recedere in tutto o in parte unilateralmente da Contratto esecutivo, con un preavviso almeno 30 (trenta) giorni solari, da comunicarsi al Fornitore tramite pec.
3. Fermo restando quanto previsto dagli artt. 88, comma 4-ter, e 92, comma 4, del D.Lgs. 159/2011, Consip S.p.A. e/o l'Amministrazione ai sensi dell'art. 109 comma 1 del Codice potrà recedere dall'Accordo Quadro e/o da ciascun singolo contratto esecutivo, in qualunque momento, con preavviso non inferiore a 20 (venti) giorni solari, previo il pagamento da parte delle Amministrazioni delle prestazioni oggetto di Contratto esecutivo eseguite a regola d'arte,

Classificazione del documento: Consip Public



nonché del valore dei materiali utili esistenti in magazzino (ove esistenti), oltre al decimo dell'importo delle opere, dei servizi o delle forniture non eseguite, ai sensi dell'art. 109 comma 2 del Codice, rinunciando espressamente il Fornitore, ora per allora, a qualsiasi ulteriore eventuale pretesa, anche di natura risarcitoria, ed a ogni ulteriore compenso e/o indennizzo e/o rimborso, anche in deroga a quanto previsto dall'articolo 1671 cod. civ..

4. Qualora la Consip receda dall'Accordo Quadro, non potranno essere affidati nuovi Contratti esecutivi da parte delle Amministrazioni e le singole Amministrazioni potranno a loro volta recedere dai singoli Contratti esecutivi, con un preavviso di almeno 30 (trenta) giorni solari, da comunicarsi al Fornitore tramite pec..

#### **ARTICOLO 16 - OBBLIGHI DERIVANTI DAL RAPPORTO DI LAVORO**

1. Il Fornitore si obbliga ad ottemperare a tutti gli obblighi verso i propri dipendenti derivanti da disposizioni legislative e regolamentari vigenti in materia di lavoro, ivi compresi quelli in tema di igiene e sicurezza, in materia previdenziale e infortunistica, assumendo a proprio carico tutti i relativi oneri. In particolare, il Fornitore si impegna a rispettare nell'esecuzione delle obbligazioni derivanti dall'Accordo Quadro e dai singoli Contratti esecutivi le disposizioni di cui al D.Lgs. 9 aprile 2008 n. 81.
2. Il Fornitore si obbliga altresì ad applicare, nei confronti dei propri dipendenti occupati nelle attività contrattuali, le condizioni normative e retributive non inferiori a quelle risultanti dai contratti collettivi ed integrativi di lavoro applicabili alla data di stipula dell'Accordo Quadro alla categoria e nelle località di svolgimento delle attività, nonché le condizioni risultanti da successive modifiche ed integrazioni, anche tenuto conto di quanto previsto all'art. 95, comma 10 e all'art. 97 del D. Lgs. n. 50/2016.
3. Il Fornitore si obbliga, altresì, fatto in ogni caso salvo il trattamento di miglior favore per il dipendente, a continuare ad applicare i suindicati contratti collettivi anche dopo la loro scadenza e fino alla loro sostituzione.
4. Gli obblighi relativi ai contratti collettivi nazionali di lavoro di cui ai commi precedenti vincolano il Fornitore anche nel caso in cui questi non aderisca alle associazioni stipulanti o receda da esse, per tutto il periodo di validità dell'Accordo Quadro e dei singoli Contratti esecutivi.
5. Restano fermi gli oneri e le responsabilità in capo al Fornitore di cui all'art. 105, comma 9, del D. Lgs. n. 50/2016 in caso di subappalto.

#### **ARTICOLO 17 - TRASPARENZA**

1. Il Fornitore espressamente ed irrevocabilmente:
  - a) dichiara che non vi è stata mediazione o altra opera di terzi per la conclusione dell'Accordo Quadro;
  - b) dichiara di non aver corrisposto né promesso di corrispondere ad alcuno, direttamente o attraverso terzi, ivi comprese le imprese collegate o controllate, somme di denaro o altra utilità a titolo di intermediazione o simili, comunque volte a facilitare la conclusione dell'Accordo Quadro stesso;
  - c) si obbliga a non versare ad alcuno, a nessun titolo, somme di danaro o altra utilità finalizzate a facilitare e/o a rendere meno onerosa l'esecuzione e/o la gestione dell'Accordo Quadro rispetto agli obblighi con esso assunti, né a compiere azioni comunque volte agli stessi fini;
  - d) si obbliga al rispetto di quanto stabilito dall'art. 42 del D.lgs. 50/2016 al fine di evitare situazioni di conflitto d'interesse.
2. Qualora non risultasse conforme al vero anche una sola delle dichiarazioni rese ai sensi del precedente comma, o il Fornitore non rispettasse per tutta la durata dell'Accordo Quadro gli impegni e gli obblighi di cui alle lettere c) e d) del precedente comma, lo stesso si intenderà risolto di diritto ai sensi e per gli effetti dell'articolo 1456 cod. civ., per fatto e colpa del Fornitore, con facoltà di Consip S.p.A. di incamerare la garanzia prestata.

Classificazione del documento: Consip Public



3. Il Fornitore si impegna al rispetto di tutte le previsioni di cui al Patto di integrità.

#### **ARTICOLO 18 - RISERVATEZZA**

1. Il Fornitore ha l'obbligo di mantenere riservati i dati e le informazioni, ivi compresi quelle che transitano per le apparecchiature di elaborazione dati, di cui venga in possesso e, comunque, a conoscenza, di non divulgarli in alcun modo e in qualsiasi forma e di non farne oggetto di utilizzazione a qualsiasi titolo per scopi diversi da quelli strettamente necessari all'esecuzione dell'Accordo Quadro e comunque per i cinque anni successivi alla cessazione di efficacia del rapporto contrattuale.
2. L'obbligo di cui al precedente comma sussiste, altresì, relativamente a tutto il materiale originario o predisposto in esecuzione dell'Accordo Quadro e degli Contratti esecutivi; tale obbligo non concerne i dati che siano o divengano di pubblico dominio.
3. Il Fornitore è responsabile per l'esatta osservanza da parte dei propri dipendenti, consulenti e collaboratori, nonché dei propri eventuali subappaltatori e dei dipendenti, consulenti e collaboratori di questi ultimi, degli obblighi di segretezza anzidetti.
4. In caso di inosservanza degli obblighi di riservatezza, le Amministrazioni e/o Consip S.p.A. hanno la facoltà di dichiarare risolto di diritto, rispettivamente, il singolo Contratto esecutivo ovvero l'Accordo Quadro, fermo restando che il Fornitore sarà tenuto a risarcire tutti i danni che dovessero derivare alle Amministrazioni e/o a Consip S.p.A..
5. Il Fornitore potrà citare i contenuti essenziali dell'Accordo Quadro e dei Contratti esecutivi affidati in proprio favore nei casi in cui ciò fosse condizione necessaria per la partecipazione del Fornitore medesimo a gare e appalti.
6. Resta fermo quanto previsto nel successivo articolo 23.

#### **ARTICOLO 19 - RESPONSABILE UNICO DELLE ATTIVITÀ CONTRATTUALI (RUAC)**

1. Il Responsabile Unico delle Attività Contrattuali (RUAC), nominato dal Fornitore è il Dott. Fabio Battelli.
2. Il RUAC è il referente responsabile nei confronti di Consip S.p.A. e/o delle Amministrazioni per l'esecuzione del presente Accordo Quadro e dei singoli Contratti esecutivi, e quindi, avrà la capacità di rappresentare ad ogni effetto il Fornitore, salvo quant'altro previsto nel Capitolato Tecnico Generale e Speciale.
3. Qualora il Fornitore dovesse trovarsi nella necessità di sostituire il RUAC, dovrà darne immediata comunicazione scritta a Consip S.p.A.

#### **ARTICOLO 20 - DIVIETO DI CESSIONE DEL CONTRATTO**

1. E' fatto assoluto divieto a ciascun Fornitore di cedere, a qualsiasi titolo, l'Accordo Quadro ed i Contratti esecutivi, a pena di nullità della cessione medesima, fatto salvo quanto previsto dall'art. 106, comma 1, lett. d), del d. lgs. n. 50/2016 e s.m.i..
2. In caso di inadempimento da parte del Fornitore degli obblighi di cui al presente articolo, Consip S.p.A. e le Amministrazioni, fermo restando il diritto al risarcimento del danno, ha facoltà di dichiarare risolto di diritto l'Accordo Quadro e i Contratti esecutivi.

#### **ARTICOLO 21 - BREVETTI INDUSTRIALI E DIRITTI D'AUTORE**

1. Il Fornitore assume ogni responsabilità conseguente all'uso di dispositivi o all'adozione di soluzioni tecniche o di altra natura che violino diritti di brevetto, di autore ed in genere di privativa altrui; il Fornitore, pertanto, si obbliga a manlevare l'Amministrazione e la Consip S.p.A., per quanto di propria competenza, dalle pretese che terzi dovessero avanzare in relazione a diritti di privativa vantati da terzi.
2. Qualora venga promossa nei confronti delle Amministrazioni e/o di Consip S.p.A. azione giudiziaria da parte di terzi

Classificazione del documento: Consip Public



che vantino diritti sulle prestazioni contrattuali, il Fornitore assume a proprio carico tutti gli oneri conseguenti, incluse le spese eventualmente sostenute per la difesa in giudizio. In questa ipotesi, l'Amministrazione e/o Consip S.p.A. sono tenute ad informare prontamente per iscritto il Fornitore in ordine alle suddette iniziative giudiziarie.

3. Nell'ipotesi di azione giudiziaria per le violazioni di cui al comma precedente tentata nei confronti di Consip S.p.A. e delle Amministrazioni e/o, le prime, fermo restando il diritto al risarcimento del danno nel caso in cui la pretesa azionata sia fondata, hanno facoltà di dichiarare la risoluzione di diritto dell'Accordo Quadro e/o dei singoli Contratti esecutivi, recuperando e/o ripetendo il corrispettivo versato, detratto un equo compenso per i servizi e/o le forniture erogati.

#### **ARTICOLO 22 - FORO COMPETENTE**

Per tutte le questioni relative ai rapporti tra il Fornitore e Consip S.p.A. inerenti il presente Accordo Quadro, sarà competente in via esclusiva il Foro di Roma.

#### **ARTICOLO 23 - TRATTAMENTO DEI DATI PERSONALI**

1. Il Fornitore dichiara di aver ricevuto prima della sottoscrizione del presente Accordo Quadro le informazioni di cui all'articolo 13 del "Regolamento UE", circa il trattamento dei dati personali, conferiti per la sottoscrizione e l'esecuzione dell'Accordo Quadro stesso e dei Contatti derivanti dagli Contratti esecutivi e di essere a conoscenza dei diritti riconosciuti ai sensi della predetta normativa. Tale informativa è contenuta nell'ambito del Capitolato d'Oneri al paragrafo 26 che deve intendersi in quest'ambito integralmente trascritto.
2. Con la sottoscrizione dell'Accordo Quadro, il rappresentante legale del Fornitore acconsente espressamente al trattamento dei dati personali come sopra definito e si impegna ad adempiere agli obblighi di rilascio dell'informativa e di richiesta del consenso, ove necessario, nei confronti delle persone fisiche interessate di cui sono forniti dati personali nell'ambito dell'esecuzione dell'Accordo Quadro e dei Contatti attuativi, per le finalità descritte nell'informativa resa nel Capitolato d'onori come sopra richiamata.
3. Le Amministrazioni Contraenti e qualsivoglia altro soggetto pubblico o privato aderendo all'Accordo Quadro, acconsentono espressamente al trattamento ed all'invio a Consip S.p.A. da parte del Fornitore e/o delle singole Amministrazioni, dei dati relativi alla fatturazione, rendicontazione e monitoraggio per le finalità connesse all'esecuzione dell'Accordo Quadro e Contratti esecutivi.
4. In adempimento agli obblighi di legge che impongono la trasparenza amministrativa (art. 1, comma 16, lett. b, e comma 32 L. 190/2012; art. 35 D. Lgs. n. 33/2013; nonché art. 29 D. Lgs. n. 50/2016), il concorrente/contraente prende atto ed acconsente a che i dati e la documentazione che la legge impone di pubblicare, siano pubblicati e diffusi, ricorrendone le condizioni, tramite il sito internet [www.consip.it](http://www.consip.it), sezione "Società Trasparente"; inoltre, il nominativo del concorrente aggiudicatario della gara ed il prezzo di aggiudicazione dell'appalto, saranno diffusi tramite i siti internet [www.acquistinretepa.it](http://www.acquistinretepa.it) e [www.mef.gov.it](http://www.mef.gov.it).
5. Con la sottoscrizione dell'Accordo Quadro ed il perfezionamento dei Contratti esecutivi, il Fornitore acconsente espressamente al trattamento dei dati personali e si impegna ad improntare il trattamento dei dati ai principi di correttezza, liceità e trasparenza nel pieno rispetto della normativa vigente (Regolamento UE 2016/679 D. Lgs. n. 196/2003 e s.m.i. e D. Lgs. n. 101/2018), ivi inclusi gli ulteriori provvedimenti, comunicati ufficiali, autorizzazioni generali, pronunce in genere emessi dall'Autorità Garante per la Protezione dei Dati Personali. In particolare, il Fornitore si impegna ad eseguire i soli trattamenti funzionali, necessari e pertinenti all'esecuzione delle prestazioni contrattuali e, in ogni modo, non incompatibili con le finalità per cui i dati sono stati raccolti.
6. Ove applicabile, in ragione dell'oggetto dell'Accordo Quadro, ove il Fornitore sia chiamato ad eseguire attività di trattamento di dati personali, il medesimo potrà essere nominato "Responsabile/sub-Responsabile del trattamento"

Classificazione del documento: Consip Public



dei dati personali ai sensi dell'art. 28 del Regolamento UE sulla base dell'atto di nomina allegato al presente Accordo Quadro. In tal caso, il Fornitore si impegna ad accettare la designazione a Responsabile/sub-Responsabile del trattamento, da parte dell'Amministrazione, relativamente ai dati personali di cui la stessa è Titolare e che potranno essere trattati dal Fornitore nell'ambito dell'erogazione dei servizi contrattualmente previsti.

7. Nel caso in cui il Fornitore violi gli obblighi previsti dalla normativa in materia di protezione dei dati personali, o nel caso di nomina a Responsabile/sub-Responsabile, agisca in modo difforme o contrario alle legittime istruzioni impartitegli dal Titolare, oppure adotti misure di sicurezza inadeguate rispetto al rischio del trattamento, risponderà integralmente del danno cagionato agli "interessati". In tal caso, l'Amministrazione potrà applicare le penali eventualmente previste nell'Accordo Quadro, e potrà risolvere il Contratto esecutivo ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno. L'Amministrazione dovrà segnalare la fattispecie alla Consip S.p.A. che potrà risolvere l'Accordo Quadro.
8. Il Fornitore si impegna ad osservare le vigenti disposizioni in materia di sicurezza e riservatezza dei dati personali e a farle osservare ai propri dipendenti e collaboratori, quali persone autorizzate al trattamento dei Dati personali.
9. In conformità a quanto previsto dal Regolamento UE/2016/679, il Fornitore dovrà garantire che i dati personali oggetto di trattamento, verranno gestiti nell'ambito dell'UE e che non sarà effettuato alcun trasferimento degli stessi verso un paese terzo o un'organizzazione internazionale al di fuori dell'UE o dello Spazio Economico Europeo, fatta eccezione dei paesi/territori/organizzazioni coperti da una decisione di adeguatezza resa dalla Commissione europea ai sensi dell'art. 45 Regolamento UE/2016/679 o da altre garanzie adeguate di cui agli artt. 46 e ss. del Regolamento stesso (es. utilizzo delle norme vincolanti d'impresa Binding Corporate Rules - BCR). Al di fuori delle predette eccezioni, il Fornitore dovrà garantire che le eventuali piattaforme/server su cui transitino i suddetti dati abbiano sede nell'UE e che qualunque replica dei dati non sia trasmessa al di fuori della UE o dello Spazio Economico Europeo.

Nel caso di servizi di assistenza/manutenzione da remoto il cui espletamento implichi comunque il trasferimento al di fuori dell'UE di tracciati di dati connessi al servizio stesso, gli eventuali dati personali contenuti nel tracciato devono essere opportunamente anonimizzati a cura del Fornitore.

Nel caso in cui all'esito di eventuali verifiche, ispezioni e audit effettuati dalla amministrazione contraente in qualità di titolare del trattamento, dovessero risultare trasferimenti di dati extra-ue in assenza delle adeguate garanzie di cui sopra, l'amministrazione diffiderà il responsabile del trattamento all'immediata interruzione del trasferimento di dati non autorizzato. In caso di mancato adeguamento a seguito della diffida, resa anche ai sensi dell'art. 1454 cc, l'amministrazione ne darà comunicazione al garante della privacy e potrà, in ragione della gravità della condotta del fornitore e fatta salva la possibilità di fissare un ulteriore termine per l'adempimento, risolvere il contratto esecutivo ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.

#### **ARTICOLO 24 - CODICE ETICO – MODELLO DI ORGANIZZAZIONE E GESTIONE EX D.LGS. N. 231/2001 - PIANO TRIENNALE PER LA PREVENZIONE DELLA CORRUZIONE E DELLA TRASPARENZA**

1. Il Fornitore dichiara di essere a conoscenza del D.Lgs. n. 231/2001 e della L. n. 190/2012 e di aver preso visione della parte generale del Modello di organizzazione, gestione e controllo, del Codice Etico, nonché del Piano triennale per la prevenzione della corruzione e della trasparenza, predisposti da Consip e pubblicati sul sito internet della Società, e di uniformarsi ai principi ivi contenuti che devono ritenersi applicabili anche nei rapporti tra il Fornitore e la Consip S.p.A.
2. Il Fornitore, per effetto della sottoscrizione del presente Accordo Quadro, promettendo anche il fatto dei propri dipendenti e/o collaboratori, si impegna: (i) ad operare nel rispetto dei principi e delle previsioni di cui al D. Lgs. n. 231/2001; (ii) ad uniformarsi alle previsioni contenute nel Modello di organizzazione, gestione e

Classificazione del documento: Consip Public





controllo adottato dalla Consip S.p.A. ai sensi della D.Lgs. n. 231/2001 per le parti di pertinenza del Fornitore medesimo nonché del Codice etico e del Piano triennale per la prevenzione della corruzione e della trasparenza per le parti di pertinenza del Fornitore medesimo.

3. In caso di inadempimento da parte del Fornitore agli obblighi di cui ai precedenti commi, la Consip S.p.A., fermo restando il diritto al risarcimento del danno, ha facoltà di dichiarare risolta di diritto il presente Accordo Quadro.

#### **ARTICOLO 25 - TRACCIABILITÀ DEI FLUSSI FINANZIARI**

1. Ai sensi e per gli effetti dell'art. 3, comma 8, della Legge 13 agosto 2010 n. 136, il Fornitore si impegna a rispettare puntualmente quanto previsto dalla predetta disposizione in ordine agli obblighi di tracciabilità dei flussi finanziari rispetto ai Contratti esecutivi.
2. Ferme restando le ulteriori ipotesi di risoluzione previste nel presente atto, si conviene che, in ogni caso, le Amministrazioni, in ottemperanza a quanto disposto dall'art. 3, comma 9 bis, della Legge 13 agosto 2010 n. 136, senza bisogno di assegnare previamente alcun termine per l'adempimento, risolveranno di diritto, ai sensi dell'art. 1456 cod. civ., nonché ai sensi dell'art. 1360 cod. civ., previa dichiarazione da comunicarsi al Fornitore con raccomandata a.r., i Contratti esecutivi nell'ipotesi in cui le transazioni siano eseguite senza avvalersi del bonifico bancario o postale ovvero degli altri documenti idonei a consentire la piena tracciabilità delle operazioni ai sensi della Legge 13 agosto 2010 n. 136 e s.m.i., del Decreto Legge 12 novembre 2010 n. 187 nonché della Determinazione dell'Autorità per la Vigilanza sui Contratti Pubblici (ora A.N.AC.) n. 8 del 18 novembre 2010.
3. In ogni caso, si conviene che Consip S.p.A., senza bisogno di assegnare previamente alcun termine per l'adempimento, si riserva di risolvere di diritto il presente Accordo Quadro, ai sensi dell'art. 1456 cod. civ., nonché ai sensi dell'art. 1360 cod. civ., previa dichiarazione da comunicarsi al Fornitore con raccomandata a.r., nell'ipotesi di reiterati inadempimenti agli obblighi di cui al precedente comma.
4. Il Fornitore è tenuto a comunicare tempestivamente e comunque entro e non oltre 7 giorni dalla/e variazione/i qualsivoglia variazione intervenuta in ordine ai dati relativi agli estremi identificativi del/i conto/i corrente/i dedicato/i nonché le generalità (nome e cognome) e il codice fiscale delle persone delegate ad operare su detto/i conto/i.
5. Il Fornitore, nella sua qualità di appaltatore, si obbliga, a mente dell'art. 3, comma 8, della Legge 13 agosto 2010 n. 136, ad inserire nei contratti eventualmente sottoscritti con i subappaltatori o i subcontraenti, a pena di nullità assoluta, una apposita clausola con la quale ciascuno di essi assume gli obblighi di tracciabilità dei flussi finanziari di cui alla Legge 13 agosto 2010 n. 136.
6. Il Fornitore, il subappaltatore o il subcontraente che ha notizia dell'inadempimento della propria controparte agli obblighi di tracciabilità finanziaria di cui all'art. 3 della Legge 13 agosto 2010 n. 136 e s.m.i è tenuto a darne immediata comunicazione a Consip S.p.A., all'Amministrazione e alla Prefettura – Ufficio Territoriale del Governo della Provincia ove ha sede la stazione appaltante.
7. Il Fornitore, si obbliga e garantisce che nei contratti sottoscritti con i subappaltatori e i subcontraenti, verrà assunta dalle predette controparti l'obbligazione specifica di risoluzione di diritto del relativo rapporto contrattuale nel caso di mancato utilizzo del bonifico bancario o postale ovvero degli strumenti idonei a consentire la piena tracciabilità dei flussi finanziari.
8. Consip S.p.A. verificherà che nei contratti di subappalto sia inserita, a pena di nullità assoluta del contratto, un'apposita clausola con la quale il subappaltatore assume gli obblighi di tracciabilità dei flussi finanziari di cui alla surrichiamata Legge. Con riferimento ai contratti di subfornitura, il Fornitore si obbliga a trasmettere alla Consip e all'Amministrazione, oltre alle informazioni di cui all'art. 105, comma 2, quinto periodo, del D. Lgs. n. 50/2016, anche

Classificazione del documento: Consip Public

Accordo Quadro avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni - ID SIGEF 2296

Accordo Quadro Lotto 2





apposita dichiarazione resa ai sensi del d.P.R. n. 445/2000, attestante che nel relativo sub-contratto, ove predisposto, sia stata inserita, a pena di nullità assoluta, un'apposita clausola con la quale il subcontraente assume gli obblighi di tracciabilità dei flussi finanziari di cui alla surrichiamata Legge, restando inteso che la Consip e/o le Amministrazioni, si riserva di procedere a verifiche a campione sulla presenza di quanto attestato, richiedendo all'uopo la produzione degli eventuali sub-contratti stipulati, e, di adottare, all'esito dell'espletata verifica ogni più opportuna determinazione, ai sensi di legge e di contratto.

9. Ai sensi della Determinazione dell'Autorità per la Vigilanza sui contratti pubblici (ora A.N.AC.) n. 10 del 22 dicembre 2010, il Fornitore, in caso di cessione dei crediti, si impegna a comunicare il/i CIG/CUP al cessionario, eventualmente anche nell'atto di cessione, affinché lo/gli stesso/i venga/no riportato/i sugli strumenti di pagamento utilizzati. Il cessionario è tenuto ad utilizzare conto/i corrente/i dedicato/i nonché ad anticipare i pagamenti al Fornitore mediante bonifico bancario o postale sul/i conto/i corrente/i dedicato/i del Fornitore medesimo riportando il CIG/CUP dallo stesso comunicato.

#### **ARTICOLO 26 - SUBAPPALTO**

1. Il Fornitore, conformemente a quanto dichiarato in sede di Offerta si è riservato di affidare in subappalto, l'esecuzione delle seguenti prestazioni:
  - Security Strategy;
  - Vulnerability Assessment;
  - Testing del codice – Statico;
  - Testing del codice – Dinamico;
  - Testing del codice – Mobile;
  - Supporto all'analisi e gestione degli incidenti;
  - Penetration Testing;
  - Compliance normativa.
2. Il subappalto, ove dichiarato in sede di offerta, sarà regolato da quanto previsto dall'art. 105 del Codice nonché dai successivi commi.
3. L'Impresa si impegna a depositare presso la Consip, almeno venti giorni prima della data di effettivo inizio dell'esecuzione delle attività oggetto del subappalto: i) l'originale o la copia autentica del contratto di subappalto che deve indicare puntualmente l'ambito operativo del subappalto sia in termini prestazionali che economici; ii) dichiarazione attestante il possesso da parte del subappaltatore dei requisiti richiesti dal Bando di gara, per lo svolgimento delle attività allo stesso affidate, ivi inclusi i requisiti di ordine generale di cui all'articolo 80 del D. Lgs. n. 50/2016; iii) la dichiarazione dell'appaltatore relativa alla sussistenza o meno di eventuali forme di controllo o collegamento a norma dell'art. 2359 c.c. con il subappaltatore; se del caso, iv) certificazione attestante il possesso da parte del subappaltatore dei requisiti di qualificazione prescritti dal D. Lgs. n. 50/2016 e s.m.i. per l'esecuzione delle attività affidate.
4. Resta inteso che l'Impresa si impegna ad inserire, nel contratto di subappalto e negli altri subcontratti, una clausola che preveda il rispetto degli obblighi di cui al Patto di Integrità da parte dei subappaltatori/subcontraenti, e la risoluzione, ai sensi dell'art. 1456 c.c., del contratto di subappalto e/o degli altri subcontratti, nel caso di violazione di tali obblighi da parte di questi ultimi; l'Impresa dovrà dare tempestiva comunicazione a Consip dell'intervenuta risoluzione.
5. In caso di mancato deposito di taluno dei suindicati documenti nel termine all'uopo previsto, la Consip S.p.A. procederà a richiedere al Fornitore l'integrazione della suddetta documentazione. Resta inteso che la suddetta



- richiesta di integrazione comporta l'interruzione del termine per la definizione del procedimento di autorizzazione del sub-appalto, che ricomincerà a decorrere dal completamento della documentazione.
6. I subappaltatori dovranno mantenere per tutta la durata del presente contratto, i requisiti richiesti per il rilascio dell'autorizzazione al subappalto. In caso di perdita dei detti requisiti la Consip revocherà l'autorizzazione.
  7. L'impresa qualora l'oggetto del subappalto subisca variazioni e l'importo dello stesso sia incrementato nonché siano variati i requisiti di qualificazione o le certificazioni deve acquisire una autorizzazione integrativa.
  8. Ai sensi dell'art. 105, comma 4, lett. a) del D. Lgs. n. 50/2016 e s.m.i. non sarà autorizzato il subappalto ad un operatore economico che abbia partecipato alla presente procedura di affidamento.
  9. Per le prestazioni affidate in subappalto:
    - A. il subappaltatore, ai sensi dell'art. 105, comma 14, del Codice, deve garantire gli stessi standard qualitativi e prestazionali previsti nel contratto di appalto e riconoscere ai lavoratori un trattamento economico e normativo non inferiore a quello che avrebbe garantito il contraente principale, inclusa l'applicazione dei medesimi contratti collettivi nazionali di lavoro, qualora le attività oggetto di subappalto coincidano con quelle caratterizzanti l'oggetto dell'appalto ovvero riguardino le lavorazioni relative alle categorie prevalenti e siano incluse nell'oggetto sociale del contraente principale;
    - B. devono essere corrisposti i costi della sicurezza e della manodopera, relativi alle prestazioni affidate in subappalto, alle imprese subappaltatrici senza alcun ribasso.
  10. L'Amministrazione contraente, sentito il direttore dell'esecuzione, provvede alla verifica dell'effettiva applicazione degli obblighi di cui al presente comma. Il Fornitore è solidalmente responsabile con il subappaltatore degli adempimenti, da parte di questo ultimo, degli obblighi di sicurezza previsti dalla normativa vigente.
  11. Il subappalto non comporta alcuna modifica agli obblighi e agli oneri del Fornitore, il quale rimane l'unico e solo responsabile, nei confronti della Consip S.p.A. e/o delle Amministrazioni Contraenti, per quanto di rispettiva competenza, della perfetta esecuzione del contratto anche per la parte subappaltata.
  12. Il Fornitore è responsabile in via esclusiva nei confronti della Consip e delle Amministrazioni Contraenti dei danni che dovessero derivare, alla Consip e alle Amministrazioni contraenti o a terzi per fatti comunque imputabili ai soggetti cui sono state affidate le suddette attività. In particolare, il Fornitore si impegna a manlevare e tenere indenne la Consip S.p.A. e/o le Amministrazioni Contraenti da qualsivoglia pretesa di terzi per fatti e colpe imputabili al subappaltatore o ai suoi ausiliari derivanti da qualsiasi perdita, danno, responsabilità, costo o spesa che possano originarsi da eventuali violazioni del Regolamento UE n. 2016/679.
  13. Il Fornitore è responsabile in solido dell'osservanza del trattamento economico e normativo stabilito dai contratti collettivi nazionale e territoriale in vigore per il settore e per la zona nella quale si eseguono le prestazioni da parte del subappaltatore nei confronti dei suoi dipendenti, per le prestazioni rese nell'ambito del subappalto. Il Fornitore trasmette alla Consip e all'Amministrazione contraente prima dell'inizio delle prestazioni la documentazione di avvenuta denuncia agli enti previdenziali, inclusa la Cassa edile, ove presente, assicurativi e antinfortunistici, nonché copia del piano della sicurezza di cui al D. Lgs. n. 81/2008. Ai fini del pagamento delle prestazioni rese nell'ambito dell'appalto o del subappalto, l'Amministrazione contraente acquisisce d'ufficio il documento unico di regolarità contributiva in corso di validità relativo a tutti i subappaltatori.
  14. L'aggiudicatario è responsabile in solido con il subappaltatore in relazione agli obblighi retributivi e contributivi, ai sensi dell'art. 29 del D. Lgs. n. 276/2003, ad eccezione del caso in cui ricorrano le fattispecie di cui all'art. 105, comma 13, lett. a) e c), del D. Lgs. n. 50/2016 e s.m.i..

Classificazione del documento: Consip Public



15. Il Fornitore si impegna a sostituire i subappaltatori relativamente ai quali apposita verifica abbia dimostrato la sussistenza dei motivi di esclusione di cui all'articolo 80 del D. Lgs. n. 50/2016 e s.m.i..
16. L'Amministrazione Contraente corrisponde direttamente al subappaltatore, al cottimista, al prestatore di servizi ed al fornitore di beni o lavori, l'importo dovuto per le prestazioni dagli stessi eseguite nei seguenti casi:  
a) quando il subappaltatore o il cottimista è una microimpresa o piccola impresa; b) in caso di inadempimento da parte dell'appaltatore; c) su richiesta del subappaltatore e se la natura del contratto lo consente. In caso contrario, salvo diversa indicazione del direttore dell'esecuzione, il Fornitore si obbliga a trasmettere all'Amministrazione contraente entro 20 giorni dalla data di ciascun pagamento da lui effettuato nei confronti dei subappaltatori, copia delle fatture quietanzate relative ai pagamenti da essa via via corrisposte al subappaltatore.
17. Nelle ipotesi di inadempimenti da parte dell'impresa subappaltatrice, ferma restando la possibilità di revoca dell'autorizzazione al subappalto, è onere del Fornitore svolgere in proprio le attività ovvero porre in essere, nei confronti del subappaltatore ogni rimedio contrattuale, ivi inclusa la risoluzione.
18. L'esecuzione delle attività subappaltate non può formare oggetto di ulteriore subappalto.
19. In caso di inadempimento da parte dell'Impresa agli obblighi di cui ai precedenti comma, la Consip e l'Amministrazione contraente possono risolvere l'AQ e il Contratto esecutivo, salvo il diritto al risarcimento del danno.
20. Solo nel caso in cui sia presente nel disciplinare di gara la clausola che vieta la partecipazione dei cd. RTI sovrabbondanti, la Consip non autorizzerà il subappalto nei casi in cui l'impresa subappaltatrice possieda singolarmente i requisiti economici e tecnici che le avrebbero consentito la partecipazione alla gara.
21. Ai sensi dell'art. 105, comma 2, del D. Lgs. n. 50/2016 e s.m.i., il Fornitore si impegna a comunicare alla Consip S.p.A., prima dell'inizio della prestazione, per tutti i sub-contratti che non sono subappalti, stipulati per l'esecuzione dell'Accordo Quadro, il nome del sub-contraente, l'importo del sub-contratto, l'oggetto del lavoro, servizio o fornitura affidati. Sono, altresì, comunicate eventuali modifiche a tali informazioni avvenute nel corso del sub-contratto.
22. Non costituiscono subappalto le fattispecie di cui al comma 3 dell'art. 105 del d. lgs. n. 50/2016 e s.m.i.. Nel caso in cui l'Impresa intenda ricorrere alle prestazioni di soggetti terzi in forza di contratti continuativi di cooperazione, servizio e/o fornitura gli stessi devono essere stati sottoscritti in epoca anteriore all'indizione della procedura finalizzata all'aggiudicazione dell'Accordo Quadro e devono essere depositati alla Consip prima o contestualmente alla sottoscrizione dell'accordo Quadro.
23. Restano fermi tutti gli obblighi e gli adempimenti previsti dall'art. 48-bis del D.P.R. 602 del 29 settembre 1973 nonché dai successivi regolamenti.
24. La Consip S.p.A., provvederà a comunicare al Casellario Informatico le informazioni di cui alla Determinazione dell'Autorità di Vigilanza sui Contratti Pubblici (ora A.N.AC) n. 1 del 10/01/2008.

#### **ARTICOLO 27 - DANNI E RESPONSABILITÀ CIVILE**

1. Il Fornitore assume in proprio ogni responsabilità per qualsiasi danno causato a persone o beni, tanto del Fornitore stesso quanto delle Amministrazioni Contraenti e/o della Consip S.p.A. e/o di terzi, in dipendenza di omissioni, negligenze o altre inadempienze relative all'esecuzione delle prestazioni che discendono dall'Accordo Quadro e ad esso riferibili, anche se eseguite da parte di terzi.

#### **ARTICOLO 28 - ONERI FISCALI E SPESE CONTRATTUALI**

1. Sono a carico del Fornitore tutti gli oneri tributari e le spese contrattuali ivi comprese quelle previste dalla normativa vigente relative all'imposta di bollo.

Classificazione del documento: Consip Public



2. Laddove la registrazione sia operata dalla Consip S.p.A. e/o dalle Amministrazioni Contraenti, le stesse comunicano al Fornitore l'importo anticipato e il conto corrente sul quale il Fornitore si impegna a versare, entro dieci giorni, l'importo anticipato. L'attestazione del versamento deve essere prodotta a Consip S.p.A. e/o alle Amministrazioni Contraenti entro venti giorni dalla data in cui è effettuato. In caso di ritardo l'importo è aumentato degli interessi legali a decorrere dalla data di scadenza del suddetto termine fino alla data di effettivo versamento.
3. Il Fornitore dichiara che le prestazioni di cui trattasi sono effettuate nell'esercizio di impresa e che trattasi di operazioni soggette all'Imposta sul Valore Aggiunto, che il Fornitore – salvo il caso di applicazione dell'art. 17-ter del d.P.R. n. 633 del 1972 introdotto dall'art. 1, comma 629, della legge n. 190 del 2014, come modificato dal D.L. 24 aprile 2017, n. 50, convertito dalla legge 21 giugno 2017, n. 96 ("split payment") - è tenuto a versare, con diritto di rivalsa, ai sensi del D.P.R. n. 633/72; conseguentemente, all'Accordo Quadro dovrà essere applicata l'imposta di registro in misura fissa, ai sensi dell'articolo 40 del D.P.R. n. 131/86, con ogni relativo onere a carico del Fornitore.

#### **ARTICOLO 29 - CONTRIBUTO A CARICO DELLE AMMINISTRAZIONI**

1. Ai sensi dell'art. 4, comma 3-quater, del D.L. 6 luglio 2012, n. 95, convertito con modificazioni in legge 7 agosto 2012, n. 135, si applica il contributo di cui all'art. 18, comma 3, D.Lgs. 1 dicembre 2009, n. 177, come disciplinato dal D.P.C.M. 23 giugno 2010.
2. Pertanto, le Amministrazioni contraenti sono tenute a versare a Consip S.p.A., entro il termine di 30 (trenta) giorni solari dalla data di perfezionamento del Contratto esecutivo, il predetto contributo nella misura prevista dall'art. 2, lettera a) (8 per mille del valore del contratto esecutivo sottoscritto se non superiore ad € 1.000.000,00) o lettera b) (5 per mille del valore del contratto esecutivo sottoscritto se superiore ad € 1.000.000,00), del D.P.C.M. 23 giugno 2010, in ragione del valore complessivo del Contratto esecutivo, determinato sulla base del Piano Operativo approvato dall'Amministrazione Beneficiaria all'atto della stipula del Contratto esecutivo medesimo.
3. In caso di incremento (entro il 20% dell'importo iniziale) del valore del Contratto esecutivo a seguito di una modifica del Piano dei Fabbisogni e del Piano Operativo approvato dall'Amministrazione contraente ai sensi del precedente articolo 6, quest'ultima è tenuta a versare a Consip S.p.A., entro il termine di 30 (trenta) giorni solari dalla predetta approvazione, un ulteriore contributo nella misura prevista dall'art. 2, lettera c), (3 per mille sull'incremento tra il valore del contratto esecutivo ed il valore dell'atto aggiuntivo) del D.P.C.M. 23 giugno 2010.
4. Le modalità operative di pagamento del predetto contributo sono rese note alle Amministrazioni contraente a mezzo di apposita comunicazione sul sito internet della Consip S.p.A. ([www.consip.it](http://www.consip.it)).
5. Il pagamento del contributo, deve essere effettuato tramite bonifico bancario sul seguente IBAN:  
Banca: Intesa San Paolo - IBAN: IT 27 X 03069 05036 100000004389; detti contributi sono considerati fuori campo dell'applicazione dell'IVA, ai sensi dell'art.2, comma 3, lettera a) del D.P.R. del 1972 e pertanto non è prevista nessuna emissione di fattura.
6. Gli stessi non rientrano nell'ambito di applicazione della tracciabilità dei flussi finanziari di cui all'articolo 3 della legge 13 agosto 2010, n. 136.

#### **ARTICOLO 30 - CLAUSOLA FINALE**

1. Il presente Accordo Quadro ed i suoi Allegati costituiscono manifestazione integrale della volontà negoziale delle parti che hanno altresì preso piena conoscenza di tutte le relative clausole, avendone negoziato il contenuto, che dichiarano quindi di approvare specificamente singolarmente nonché nel loro insieme e, comunque, qualunque modifica al presente atto ed ai suoi Allegati non potrà aver luogo e non potrà essere provata che mediante atto scritto; inoltre, l'eventuale invalidità o inefficacia di una delle clausole dell'Accordo Quadro e/o dei singoli Contratti esecutivi non comporta l'invalidità o inefficacia dei medesimi atti nel loro complesso.

Classificazione del documento: Consip Public



2. Qualsiasi omissioni o ritardo nella richiesta di adempimento dell'Accordo Quadro o dei singoli Contratti esecutivi (o di parte di essi) da parte di Consip S.p.A. e/o delle Amministrazioni non costituisce in nessun caso rinuncia ai diritti loro spettanti che le medesime si riservano comunque di far valere nei limiti della prescrizione.
3. Con il presente Accordo Quadro si intendono regolati tutti i termini generali del rapporto tra le Parti; in conseguenza esso non verrà sostituito o superato dai Contratti esecutivi o integrativi dell'Accordo Quadro che sopravvivrà ai detti Contratti esecutivi continuando, con essi, a regolare la materia tra le Parti.

#### **ART. 31 – PENDENZA TERMINE APPELLO SU SENTENZA TAR LAZIO**

1. Atteso che, la stipula avviene in pendenza del termine per la proposizione dell'appello avverso la sentenza del TAR Lazio Roma n. 04840/2022, che ha confermato la piena legittimità del provvedimento di aggiudicazione disposto dalla Consip S.p.A. in favore del Fornitore e che, dalla proposizione di tale gravame potrebbe derivare un eventuale e futuro provvedimento giurisdizionale e/o amministrativo relativo a ulteriori e diversi giudizi o procedimenti di qualsivoglia natura che dovessero essere instaurati da chicchessia – qualora dovesse essere imposto il riesame e/o l'annullamento, anche in autotutela, dell'aggiudicazione definitiva e/o della gara e da ciò scaturisse qualsiasi tipo di invalidità e/o perdita di efficacia del contratto, il Fornitore con la sottoscrizione del contratto espressamente rinuncia, ora per allora, irrevocabilmente ed a titolo definitivo, a proporre successive azioni e/o eccezioni volte ad ottenere un risarcimento del danno nei confronti della stazione appaltante. Restano salvi ed impregiudicati i diritti del Fornitore all'impugnativa dei provvedimenti giudiziali e/o amministrativi che lo vedessero soccombente nei procedimenti giudiziari di cui sopra.

Roma, lì

**CONSIP S.p.A.**

**IL FORNITORE**

---

---

Il sottoscritto, nella qualità di legale rappresentante del Fornitore, dichiara di avere particolareggiata e perfetta conoscenza di tutte le clausole contrattuali e dei documenti ed atti ivi richiamati; ai sensi e per gli effetti di cui agli artt. 1341 e 1342 cod. civ., il Fornitore dichiara di accettare tutte le condizioni e patti ivi contenuti e di avere particolarmente considerato quanto stabilito e convenuto con le relative clausole; in particolare dichiara di approvare specificamente le clausole e condizioni di seguito elencate:

Articolo 3 (Oggetto dell'Accordo Quadro), Articolo 4 (Durata dell'Accordo Quadro e dei Contratti esecutivi), Articolo 5 (Prezzi e vincoli dei Contratti esecutivi), Articolo 6 (Affidamento dei Contratti esecutivi), Articolo 7 (Obbligazioni generali del Fornitore), Articolo 8 (Obbligazioni specifiche del Fornitore), Articolo 9 (Verifica di conformità), Articolo 10 (Corrispettivi e fatturazione), Articolo 11 (Costi della sicurezza); Articolo 12 (Penali); Articolo 13 (Garanzie); Articolo 14 (Risoluzione); Articolo 15 (Recesso); Articolo 16 (Obblighi derivanti dal rapporto di lavoro), Articolo 17 (Trasparenza), Articolo 18 (Riservatezza), Articolo 19 (Responsabile Unico delle Attività Contrattuali), Articolo 20 (Divieto di cessione del contratto), Articolo 21 (Brevetti industriali e diritti d'autore); Articolo 22 (Foro competente); Articolo 23 (Trattamento dei dati personali); Articolo 24 (Codice Etico – Modello di organizzazione e gestione ex D.Lgs. n. 231/2001 – Piano Triennale per la prevenzione della corruzione e della trasparenza), Articolo 25 (Tracciabilità dei flussi finanziari), Articolo 26 (Subappalto), Articolo 27 (Danni e responsabilità civile), Articolo 28 (Oneri fiscali e spese contrattuali), Articolo 29

Classificazione del documento: Consip Public



(Commissione a carico delle Amministrazioni), Art. 30 (Clausola finale), Articolo 31 (Pendenza termine appello su sentenza TAR Lazio).

Roma, li \_\_\_\_ \_\_\_\_

**IL FORNITORE**

Classificazione del documento: Consip Public

Accordo Quadro avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni - ID SIGEF 2296

Accordo Quadro Lotto 2

## **ALLEGATO A – OFFERTA TECNICA DEL FORNITORE**



**GARA A PROCEDURA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L’AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI – ID 2296 LOTTO 2**

## ***Relazione Tecnica***



**INDICE**

<b>1</b>	<b>PREMESSA.....</b>	<b>1</b>
<b>2</b>	<b>PRESENTAZIONE E DESCRIZIONE OFFERENTE .....</b>	<b>1</b>
<b>3</b>	<b>STRUTTURA ORGANIZZATIVA.....</b>	<b>2</b>
3.1	MODALITÀ ORGANIZZATIVE ED ORGANIGRAMMA (AQ-ACCORDO QUADRO E CE-CONTRATTI ESECUTIVI).....	2
3.2	DISTRIBUZIONE DELLE RESPONSABILITÀ E PROCEDURE DI COORDINAMENTO .....	3
3.3	RUOLI, RISORSE E STRUTTURE AGGIUNTIVI PROPOSTI PER LA GESTIONE FORNITURA E MODALITÀ DI INTERAZIONE CON L'AMMINISTRAZIONE .....	4
<b>4</b>	<b>PROPOSTA PROGETTUALE PER IL SERVIZIO "SECURITY STRATEGY" .....</b>	<b>5</b>
4.1	PROPOSTA DI ELABORAZIONE DEL PROGETTO DI SICUREZZA E MODELLO CORRELAZIONE DEI SERVIZI.....	5
4.2	PROPOSTA DI ELABORAZIONE DI UN MODELLO DI ANALISI DEI FABBISOGNI DI BENI E SERVIZI DI SICUREZZA.....	7
4.3	TEAM DI LAVORO .....	8
<b>5</b>	<b>PROPOSTA PROGETTUALE PER IL SERVIZIO "VULNERABILITY ASSESSMENT" .....</b>	<b>9</b>
5.1	MODALITÀ DI ESECUZIONE DEL SERVIZIO.....	9
5.2	PROPOSTA DI REMEDIATION PLAN E REPORTISTICA DI SINTESI E DETTAGLIO.....	10
5.3	TEAM DI LAVORO .....	11
<b>6</b>	<b>PROPOSTA PROGETTUALE PER I SERVIZI "TESTING DEL CODICE" .....</b>	<b>11</b>
6.1	MODALITÀ DI ESECUZIONE DEL SERVIZIO.....	11
6.2	PROPOSTA DI REMEDIATION PLAN E REPORTISTICA DI SINTESI E DETTAGLIO .....	13
6.3	MODALITÀ DI INTEGRAZIONE COL REPOSITORY SOFTWARE.....	13
<b>7</b>	<b>PROPOSTA PROGETTUALE PER IL SERVIZIO "SUPPORTO ALL'ANALISI E GESTIONE DEGLI INCIDENTI" .....</b>	<b>14</b>
7.1	MODALITÀ DI ESECUZIONE DEL SERVIZIO, MODELLO ORGANIZZATIVO ADOTTATO E STRUMENTI.....	14
7.2	PROPOSTA DEL DOCUMENTO DI CATENA DI CUSTODIA .....	16
7.3	TEAM DI LAVORO .....	17
<b>8</b>	<b>PROPOSTA PROGETTUALE PER IL SERVIZIO "PENETRATION TESTING" .....</b>	<b>17</b>
8.1	MODALITÀ DI ESECUZIONE DEL SERVIZIO E CAUTELE ADOTTATE .....	17
8.2	PROPOSTA DI DELIVERABLE DOCUMENTALI .....	19
8.3	TEAM DI LAVORO .....	19
<b>9</b>	<b>PROPOSTA PROGETTUALE PER IL SERVIZIO "COMPLIANCE NORMATIVA" .....</b>	<b>19</b>
9.1	MODALITÀ DI ESECUZIONE DEL SERVIZIO, AMBITI DI INTERVENTO, MODELLO ORGANIZZATIVO E STRUMENTI.....	20
9.2	PROPOSTA DI RAPPORTO DI COMPLIANCE.....	22
9.3	TEAM DI LAVORO .....	22
<b>10</b>	<b>PORTALE DELLA FORNITURA.....</b>	<b>23</b>
10.1	SOLUZIONI TECNOLOGICHE E FUNZIONALITÀ PROPOSTE.....	23
10.2	STRUMENTI DI ANALISI DEI DATI E REPORTING .....	24
10.3	SOLUZIONI, PROCESSI E STRUMENTI DI COMUNICAZIONE E DI COLLABORAZIONE IN CHIAVE "SOCIAL" .....	25
<b>11</b>	<b>MIGLIORAMENTO SOGLIE INDICATORI DI QUALITÀ – RLFN – Rilievi sulla fornitura .....</b>	<b>25</b>
<b>12</b>	<b>MIGLIORAMENTO SOGLIE INDICATORI DI QUALITÀ – SLSC – Rispetto di una scadenza contrattuale .....</b>	<b>25</b>
<b>13</b>	<b>MIGLIORAMENTO SOGLIE INDICATORI DI QUALITÀ – NAPP – Non approvazione di documenti.....</b>	<b>25</b>
<b>14</b>	<b>INNOVAZIONE .....</b>	<b>25</b>
14.1	SOGGETTI COINVOLTI E LORO PRINCIPALI CARATTERISTICHE.....	25
14.2	AMBITO DI INTERVENTO E VALORE AGGIUNTO APPORTATO.....	26
14.3	MODALITÀ ORGANIZZATIVE DEL COINVOLGIMENTO .....	27
<b>15</b>	<b>FLESSIBILITÀ DELLE RISORSE .....</b>	<b>27</b>
15.1	DISPONIBILITÀ E TEMPESTIVITÀ DI ALLOCAZIONE DELLE RISORSE PROFESSIONALI .....	28
15.2	METODOLOGIE E STRUMENTI PROPOSTI PER LA FLESSIBILITÀ NELLA GESTIONE DI PIÙ CONTRATTI IN CONTEMPORANEA .....	28
<b>16</b>	<b>AGGIORNAMENTO DELLE RISORSE PROFESSIONALI .....</b>	<b>29</b>
16.1	SOLUZIONI PROGETTUALI E STRUMENTI PER GARANTIRE LA FORMAZIONE E L'AGGIORNAMENTO CONTINUO.....	29
16.2	PROPOSTA DI PIANO FORMATIVO .....	30
<b>17</b>	<b>ASSUNZIONE DELLE RISORSE PROFESSIONALI.....</b>	<b>30</b>


## 1 PREMESSA

Il presente documento rappresenta la Relazione Tecnica redatta dal RTI composto da Deloitte Risk Advisory S.r.l., EY Advisory S.p.A. e Teleco, per la "Gara a procedura aperta per la conclusione di un accordo quadro, ai sensi del D.Lgs. 50/2016 e s.m.i., suddivisa in 2 lotti e avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni – ID 2296 – Lotto 2". La Relazione Tecnica capitalizza la conoscenza del contesto pubblico e le molteplici esperienze maturate dal RTI sulle tematiche di servizi di sicurezza da remoto, di compliance e controllo, nonché le esperienze delle aziende del RTI a supporto della stessa Agenzia per l'Italia Digitale. **Per facilitare la lettura, gli Allegati A e B forniscono rispettivamente le immagini in formato sorgente e gli acronimi utilizzati nel presente documento.**

## 2 PRESENTAZIONE E DESCRIZIONE OFFERENTE

**Deloitte.** Deloitte Risk Advisory S.r.l. (di seguito DRA) fa parte della realtà Deloitte Italia con **più di 7.700 dipendenti** e 340.000 nel mondo con presenza in oltre 150 Paesi. La divisione **Cyber Risk Services** conta **circa 350 professionisti in Italia**. Il portafoglio **Cyber Security** di Deloitte copre tutti gli aspetti relativi alla riduzione dei rischi informatici dei propri clienti; ciò si compie attraverso servizi di Cyber Strategy, Detect & Respond, Application Security, Cyber Cloud, Infrastructure Security, Industrial & Product Security, Data & Privacy ed Identity. I professionisti di DRA sono distribuiti nelle sedi operative di Bari, Bologna, Firenze, Genova, Milano, Padova, Roma, Torino garantendo un **importante presidio in tutto il territorio italiano** al RTI nel suo complesso. Il business Cyber di Deloitte è costruito mediante un **Global Network** mondiale che conta più di 8.600 professionisti dedicati ai servizi di Cyber Risk coadiuvati da ulteriori **10.000+ risorse** di altre aree focalizzate sui temi di security. Deloitte vanta inoltre più di **30 Cyber Intelligence Center** che forniscono servizi di consulenza sui temi SOC, realizzano soluzioni di sicurezza gestite completamente personalizzabili, tra cui il monitoraggio avanzato della sicurezza, l'analisi e la gestione delle minacce cyber e la risposta agli incidenti per le aziende-clienti. Tutti i servizi sono erogati garantendo metodologie ed approcci ottimizzati e comuni, profonda attenzione ai livelli di qualità dei deliverable, soluzioni e strumenti operativi in continua evoluzione e un insieme globale di punti di osservazione della trasformazione digitale della Pubblica Amministrazione sia italiana che internazionale. Deloitte è stata nominata **Leader** tra i **Cybersecurity Consulting Provider Europei** da Forrester Wave, per il terzo trimestre 2021 e, per il **decimo anno consecutivo**, si è classificata come **Leader** per **Security Consulting Services Worldwide** da Gartner (2020).

 **EY Advisory S.p.A.** (di seguito EYA) fa parte della realtà EY Italia con **più di 5.000 dipendenti**, 312.000 nel mondo con presenza in 150 paesi. La divisione **Cybersecurity & Digital Protection**, all'interno di EY, conta **più di 200 professionisti in Italia** a supporto di clienti nazionali ed internazionali sulle tematiche di Cyber Strategy Risk Compliance & Resilience, Data Protection & Privacy, Identity & Access Management, Cyber Architecture Engineering & Emerging Technology e Next Generation Security Operations & Response. Tali professionisti appartengono alle sedi operative di Bari, Bologna, Milano, Roma, Torino e Treviso, garantendo **presenza capillare sul territorio nazionale** al RTI nel suo complesso. Il **Network mondiale EY Cybersecurity** è costituito da più di 14.000 risorse che si avvalgono di un insieme comune di metodologie, asset e approcci di settore, a garanzia di qualità dei deliverable, strumenti operativi consolidati e visione privilegiata sulle evoluzioni del settore Pubblico anche a livello internazionale. EY vanta inoltre più di **60 Cybersecurity Center** e **12 Advanced Security Center** che forniscono servizi innovativi di sicurezza avvalendosi di soluzioni tecnologiche all'avanguardia. EY è stata nominata **Leader** tra i **Cybersecurity Consulting Provider Europei** da Forrester Wave (Luglio 2021) e Market Share Analysis Leader per i **Security Consulting Services Worldwide** da Gartner (Giugno 2021).

 **TELECO S.r.l.** (di seguito TEL) è una **PMI Innovativa**, registrata in CCIAA Roma al N. 220439/2019 e iscritta al MISE – Ministero dello Sviluppo Economico, che sviluppa attività di Ricerca & Sviluppo in ambito Sicurezza Informatica e Privacy, Vulnerability Assessment, Penetration Test, Application Security riferito anche ad ambienti ICS, OT, IoT ed utilizzando tecnologie innovative (BigData-Analytics). Dispone di una sede legale e operativa in Roma e un **Polo Tecnologico** in Cagliari con oltre 50 dipendenti tra quadri e figure operative con competenze trasversali, ai quali si uniscono società partner per il raggiungimento su base progetto di una disponibilità di oltre 100 risorse, garantendo la presenza sull'intero territorio nazionale. Fondata nel 1999, opera anche come System Integrator con focalizzazione ad una clientela nel settore della Pubblica Amministrazione Centrale e Locale (Centro-Sud).

**Indicazione dei dati identificativi dei soggetti muniti dei necessari poteri che sottoscrive l'offerta per il concorrente.**

- **Deloitte Risk Advisory S.r.l.:** **Lorenzo Fersurella**, nato a Taranto (TA) il 15/08/74 (C.F. FRSLN274M15L049G), domiciliato per la carica presso la sede societaria in Milano, Via Tortona n. 25 – CAP 20144, nella sua qualità di Procuratore
- **EY Advisory S.p.A.:** **Dario Bergamo**, nato a Scalea (CS) il 25/08/1964 (C.F. BRGDRA64M25I489L), domiciliato per la carica presso la sede societaria in Milano, Via Meravigli n. 14 – CAP 20123, nella sua qualità di Procuratore Speciale
- **Teleco S.r.l.:** **Fiorenzo Trogu**, nato a Cagliari (CA) il 21/10/53 (C.F. TRGFNZ53R21B354O), domiciliato per la carica presso la sede societaria in Roma, Via Rosazza n.26, nella sua qualità di Presidente del Consiglio di Amministrazione

**Organizzazione adottata per la distribuzione dei servizi/attività tra le aziende partecipanti.** Il RTI è stato ideato con l'intenzione di mettere a disposizione delle Amministrazioni che aderiranno al presente Lotto, un **paniere esaustivo e "unico" di competenze multidisciplinari e complementari**. Le stesse sono funzionali ad assicurare una **gestione integrata, qualificata e orientata alla frontiera dell'innovazione in ambito Cybersecurity** di tutti i servizi oggetto di fornitura, garantendo un **elevato presidio delle Amministrazioni Centrali e Locali**, attraverso i rispettivi **uffici territoriali, grazie alla presenza di molteplici sedi operative dislocate sull'intero territorio nazionale**. In tale ottica, le aziende del RTI operano nella Fornitura in sinergia con i team specialistici (§3.2). Nel complesso le aziende assicurano la capacità di governo dell'Accordo Quadro e dei Contratti Esecutivi. DRA e EYA hanno perseguito un percorso di specializzazione differente che ha portato **DRA** a focalizzarsi maggiormente sugli ambiti Operations e Verifiche tecniche, mentre **EYA** sugli ambiti Strategy e Compliance. Per tale motivo, DRA avrà maggior prevalenza sulle attività di Vulnerability Assessment, Testing del Codice, Penetration Testing e Supporto Incidenti; mentre EYA sulle attività di Strategy e Compliance. **TEL (PMI Innovativa - Aut. MISE 220439)**, coinvolta nel RTI al fine di valorizzare l'innovazione nell'esecuzione su specifici servizi. Il coinvolgimento sarà nelle attività di ricerca e sviluppo funzionali ad elaborare soluzioni ed approcci metodologici innovativi, in particolare per le attività di Testing del Codice e Penetration Test in **ambienti tecnologici emergenti** (Cloud Computing, Big Data & Analytics, 3D User Experience, Internet of Things, Smart

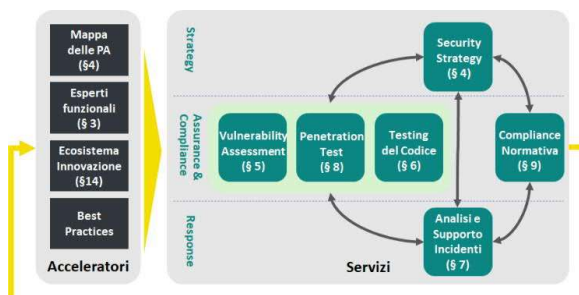
& Intelligent Building). Tali tecnologie potranno trovare applicazione ai servizi del Lotto 2 anche allo scopo di contribuire a qualità e innovazione dei servizi in ambito (§14).

### 3 STRUTTURA ORGANIZZATIVA

**1. La comprovata esperienza del RTI su contratti analoghi** ha consentito di progettare un modello “ad hoc” per l'erogazione dei servizi verso tipologie di Amministrazioni fortemente eterogenee **2. Governance, flessibilità e specializzazione garantita da una Organizzazione strutturata su 5 livelli con 17 ruoli/figure aggiuntive.** **3. Efficace ed efficiente modalità di interazione** tra le strutture del RTI, volta a garantire *readiness* e omogeneità nell'erogazione dei servizi. **4. Processo sistematico ed indipendente di Quality Assurance, da parte di esperti nazionali ed internazionali,** a garanzia di un elevato livello dei servizi e rispetto dei più stringenti standard di qualità.

**3.1 MODALITÀ ORGANIZZATIVE ED ORGANIGRAMMA (AQ-ACCORDO QUADRO E CE-CONTRATTI ESECUTIVI).** Con l'obiettivo di una più efficiente ed efficace erogazione dei servizi di fornitura, valorizzando esperienze su contratti paragonabili, il RTI ha definito un **modello operativo ad hoc per la fornitura** che rappresenta l'**approccio strutturato del RTI all'erogazione dei servizi**. Il modello è costituito da due livelli:

**Acceleratori:** questo livello è composto da tutti gli strumenti messi a disposizione dal RTI che garantiscono un continuo input ai servizi dei CE in termini di valorizzazione degli esperti tematici e di **settore** (§ 3.1) e delle strutture preposte all'**innovazione** (§ 14) e di **capitalizzazione** delle best practices (§ da 4 a 9). A questo livello è mantenuta la **MappaPA** (§ 4) che garantisce, grazie a un lavoro preprogettuale di classificazione delle Amministrazioni



in tipologie omogenee sulla base delle caratteristiche e dei profili di rischio delle stesse, di avere sempre a disposizione modelli predefiniti da personalizzare per ciascun CE. La MappaPA sarà pubblicata all'interno del Portale della Fornitura. **Servizi:** a questo livello il RTI ha definito un modello di interazione tra i servizi (§ da 4 a 9) che ne garantisce le sinergie, valorizzandone i risultati. Tale modello è alimentato dagli input ricevuti a livello di CE sia in termini di competenze e capitalizzazione delle esperienze, sia attraverso la guida fornita dalla MappaPA per la scelta e l'utilizzo di metodologie, tecniche e soluzioni più adatte. In un'ottica di miglioramento continuo i risultati a livello di CE costituiranno input di valore per gli Organismi di Coordinamento e Controllo.

**3.1.1 Struttura organizzativa dedicata per la gestione di AQ e CE.** L'organizzazione proposta dal RTI è **strutturata su 5 livelli** per garantire una **efficace**

**governance** a livello di AQ e CE, è arricchita da figure con **competenze tematiche e dominio** che assicurano una completa copertura tecnica e funzionale, prevede il **coinvolgimento di risorse e strutture innovative** con l'obiettivo di garantire un costante **allineamento con le trasformazioni del mercato**. Le responsabilità sono distribuite tra le unità operative del RTI e sono previste figure/unità aggiuntive offerte senza alcun onere (★) per le Amministrazioni aderenti all'AQ.

**GOVERNO AQ:** A questo livello risiede la governance, la programmazione e il monitoraggio dell'intero AQ. I ruoli

di questo livello: **RUAC AQ** figura dirigenziale con esperienza pluriennale nella governance di programmi di trasformazione in ambito Cybersecurity. Adempie agli obblighi di cui all'Appendice 1 del CTG (par. 2.2) e assicura la guida dell'AQ garantendo, a Consip e agli Organismi di Coordinamento e Controllo (OCC), un'omogeneità di approccio su ciascun CE; definisce gli indirizzi strategici a livello di AQ e verifica l'aderenza dei singoli CE agli stessi. Presiede il Board del RTI composto da un profilo di vertice di ciascuna componente. Nelle attività il RUAC è coadiuvato dalla struttura **Funzioni di Supporto (FdS)** che è composta da:

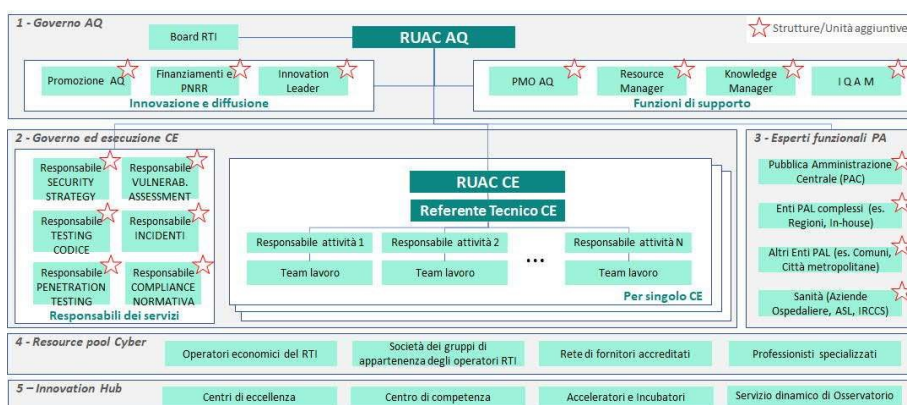
→ **PMO AQ** (★) Pianifica e monitora l'avanzamento complessivo dell'AQ, assicurando al contempo omogeneità di standard qualitativi (adottati a livello di CE) e di approccio nella definizione dei documenti di pianificazione e stato avanzamento lavori (SAL). Supporta operativamente il RUAC nelle attività di elaborazione della reportistica di monitoraggio dell'AQ da mettere a disposizione di Consip e OCC.

→ **Resource Manager RM** (★) Gestisce centralmente il processo di staffing dei professionisti del RTI all'interno dei team di intervento sui diversi CE, individuando le professionalità più idonee per soddisfare i fabbisogni di supporto e innovazione. Gestisce a livello di AQ i processi di allocazione, ottimizzando le trasferte dei professionisti del RTI rispetto alle sedi di erogazione dei Servizi.

→ **Knowledge Manager KM** (★) assicura la valorizzazione e il riutilizzo del patrimonio di best practices e “lesson learned” acquisite durante la fornitura anche attraverso la formazione e l'aggiornamento continuo delle risorse del RTI di cui è responsabile (§ 16). → **IQAM** (★) il RTI prevede il coinvolgimento di una figura esterna al team (Independent Quality Assurance Manager– IQAM), di profilo internazionale sui progetti più significativi allo scopo di garantire un rigido processo di quality review indipendente (Service Quality Program), che prevede sui singoli progetti previsti dal Lotto, una sistematica revisione delle attività svolte e che ha l'obiettivo di recepire e monitorare il livello di soddisfazione del cliente instaurando una relazione indipendente con esso. In staff al RUAC è prevista una ulteriore struttura di **Innovazione e Diffusione (I&D)** così composta: → **Promozione AQ** (★) promuove la diffusione dell'AQ tramite iniziative e seminari per assicurare il massimo livello di adesione delle PA interessate e supportandole nelle fasi operative di adesione all'AQ. → **Finanziamenti e PNRR** (★)

supporta le Amministrazioni nell'identificazione di fonti di finanziamento (es. PNRR o altri fondi comunitari e nazionali) per i progetti nell'ambito dei CE. → **Innovation Leader** (★) ingaggia sul singolo CE le strutture dell'ecosistema interno ed esterno (Innovation Hub) più idonee alle esigenze di ciascun CE per assicurare la migliore risposta in termini di soluzione innovative contribuendo all'evoluzione continua del sistema di protezione del comparto.

**GOVERNO ED ESECUZIONE CE:** questo livello gestisce l'erogazione dei CE in linea con le strategie definite a livello di AQ. I ruoli di questo livello: → **Responsabili**



**dei Servizi (RdS ★):** per ciascun servizio è individuato un responsabile che supporta i Referenti Tecnici dei CE assicurando omogeneità di approccio trasversalmente alle diverse Amministrazioni e abilitando il riuso delle soluzioni già applicate con successo su altri CE. → **RUAC CE:** figura responsabile dell'attuazione del CE, rappresenta il RTI nei confronti della singola Amministrazione. → **Referente Tecnico CE (RT)** per l'erogazione dei servizi, referente tecnico per ciascun CE e comunque per ciascuna Amministrazione per tutti i servizi del Lotto 2, assicurando il corretto svolgimento dei servizi ed il relativo livello di qualità di erogazione, nel pieno rispetto degli indicatori condivisi. Ha la responsabilità delle attività di Presa in carico e trasferimento di Know How durante le quali è il riferimento per il fornitore uscente/entrante e coordina le attività dei team di lavoro. → **Responsabile Attività** referente tecnico per ciascuna attività all'interno del CE, coordina e assicura il corretto svolgimento delle attività operative eseguite dal team di lavoro; il ruolo è ricoperto dalla risorsa del team di lavoro con maggiore esperienza professionale. → **Team di Lavoro (TL)**, team operativi di intervento impegnati nell'erogazione dei servizi, composti da professionisti con profili previsti dall'Appendice 2 – Profili Professionali.

**ESPERTI FUNZIONALI PA (EFPA):** questo livello è composto dagli esperti di contesto delle Amministrazioni e garantisce un supporto ai team di CE in termini di contestualizzazione rispetto ai cluster di Amministrazioni aderenti. I ruoli di questo livello: → **Esperti funzionali della PA (★)** 4 referenti coadiuvati da figure di supporto, responsabili delle tematiche di sicurezza in rispetto alla MappaPA individuata dal RTI. Le 4 tipologie individuate dal RTI sono: 1) PAC, 2) Enti locali complessi come Regioni e In-house, 3) Altri Enti locali come Comuni, Città metropolitane, 4) Amministrazioni in ambito Sanitario.

**RESOURCE POOL CYBER (RPC):** Livello composto da un pool di professionisti appartenenti agli operatori economici del RTI e delle società dei rispettivi gruppi di appartenenza, rete di fornitori accreditati e professionisti specializzati, assicurando la necessaria copertura in termini di competenze e volumi per soddisfare le esigenze delle Amministrazioni, anche rispetto della contemporaneità delle richieste. Le risorse sono allocate dal Resource manager all'interno dei team di lavoro nell'ambito del singolo CE.

**INNOVATION HUB (IH):** Livello composto dall'insieme di strutture operative coinvolte nel corso della Fornitura attraverso l'Innovation Leader (§ 14). Quest'ultimo seleziona ed ingaggia, sulla base delle tematiche di interesse, le strutture più idonee per apportare contributi a valore aggiunto per l'innovazione e la trasformazione in ambito Cybersecurity delle Amministrazioni. La capacità di supportare l'innovazione su ogni CE è garantita dall'utilizzo di un ecosistema dell'Innovazione interno ed esterno (§ 14) basato su: → **Centri di eccellenza** dedicati ai temi di innovazione in ambito ICT tecnologie e digital, → **Centro di competenza** che mettono a disposizione dei Team conoscenze specialistiche, metodologie e soluzioni e tool innovativi – consolidati dai network nazionali ed internazionali del RTI – in grado di aumentare la qualità e l'efficacia dei servizi, → **Acceleratori e Incubatori**, strutture afferenti al RTI che sostengono e accelerano la crescita di start-up e PMI innovative, attraverso strumenti ad hoc (es. business matching e networking, accesso a opportunità di finanziamento, nuovi mercati e alla finanza agevolata), → **Servizio dinamico di Osservatorio** delle startup sugli acceleratori e sulle competenze in ambito cybersecurity abilitato da numerose iniziative che presidiano la frontiera dell'innovazione su temi Cyber in particolare.

**3.2 DISTRIBUZIONE DELLE RESPONSABILITÀ E PROCEDURE DI COORDINAMENTO.** In considerazione della complessità della Fornitura dei servizi oggetto del Lotto 2 ed allo scopo di strutturare il modello di interazione tra le strutture interne in maniera efficace ed efficiente ai fini dell'erogazione dei servizi verso le amministrazioni, il RTI ha definito: un **apposito modello per la distribuzione delle responsabilità** tra i componenti del RTI, **dei puntuali meccanismi di interazione tra le strutture operative e di governance** dell'AQ, delle **procedure di coordinamento** volte a facilitare la collaborazione tra i team operativi (strutture interne) e le aziende raggruppate e un **approccio di presa in carico** per garantire rapidità ed efficacia nell'attivazione dei servizi.

#### MODELLO DI DISTRIBUZIONE DELLE RESPONSABILITÀ

Il RTI ha definito sin dalla fase di offerta una chiara assegnazione del livello di coinvolgimento di ogni componente del costituendo RTI. DRA e EYA hanno perseguito un percorso di specializzazione differente che ha portato DRA a focalizzarsi maggiormente sugli ambiti Operations e Verifiche tecniche, mentre EYA sugli ambiti Strategy e Compliance. Per tale motivo, DRA avrà maggior prevalenza sulle attività di Vulnerability Assessment, Testing del Codice, Penetration Testing e Supporto Incidenti; mentre EYA sulle attività di Strategy e Compliance. TEL (PMI Innovativa) è coinvolta nel RTI al fine di valorizzare l'innovazione nell'esecuzione su specifici servizi. Il coinvolgimento sarà nelle attività di ricerca e sviluppo funzionali ad elaborare soluzioni ed approcci metodologici innovativi, in particolare per le attività di Testing del Codice e Penetration Test in ambienti tecnologici emergenti (Cloud

Computing, Big Data & Analytics, 3D User Experience, Internet of Things, Smart & Intelligent Building). Tali tecnologie potranno trovare applicazione ai servizi del Lotto 2 anche allo scopo di contribuire a qualità e innovazione dei servizi in ambito.

**Legenda:** Livello di coinvolgimento delle aziende partecipanti

Molto Basso ○ Basso ◐ Medio ◑ Medio-Alto ◒ Alto ●

SERVIZI	RIPARTIZIONE PER AZIENDA		
	DLT	EYA	TEL
Security Strategy	◑	●	○
Vulnerability Assessment	●	◑	◐
Testing del codice	●	◐	◑
Supporto analisi e gestione incidenti	●	◐	◐
Penetration Testing	●	◑	◑
Compliance normativa	◐	●	◐

Il RTI potrà inoltre coinvolgere nell'ambito di una collaborazione continuativa la **Fondazione Bruno Kessler, Ente di Ricerca** specializzato in cybersecurity, per lo sviluppo di metodologie ed approcci a fronte di evoluzioni normative, cambiamenti di scenario tecnologico ed evoluzione del sistema di cybersecurity. Si riporta inoltre qui di seguito uno schema sintetico che indica **la matrice RACI relativa alle differenti fasi previste a livello di AQ e CE**. Tale soluzione è volta ad assicurare efficacia e concretezza di erogazione ed è pienamente basata sulla piena collaborazione tra i diversi ruoli e livelli dell'organizzazione.

	FASE	RUAC	PMO	RM	KM	IQAM	I&D	RUAC	RT	RdS	TL	RPC	EFPA	IH
AQ	Indirizzo Strategico	A/R	I				C	I					C	C
	Allocazione Risorse	A		R				R	C	C		C		C
	Gestione della conoscenza & Best Practice	C			A/R		I	I	I	C	C		C	C
	Gestione Piano della Qualità Generale	A/R				R		I	I					
	Gestione Portale	C			A/R			C	I					
CE	Piano Operativo & Orchestrazione Servizi	I	I				C	A	R	C	I	C	C	C
	Presa in carico & Trasferimento Know-how	I	C		C			C	A/R	C	C			



FASE	RUAC	PMO	RM	KM	IQAM	I&D	RUAC	RT	RdS	TL	RPC	EFPA	IH
Gestione Piano della Qualità Specifico CE	I				R		A/R	R		R			
Erogazione Servizi Oggetto della fornitura		C					I	A/R	C	R	C	C	R
Monitoraggio KPI e rilievi sulla fornitura	I	C					A	R					

**MECCANISMI DI INTERAZIONE TRA LE STRUTTURE OPERATIVE E DI GOVERNANCE:** Per ciascuna delle aeree presidiate, il RTI ha concretamente identificato modalità di interazione, attività, risultati immediatamente tangibili e momenti puntuali di confronto in relazione ai ruoli organizzativi identificati.

	FASE	ATTIVITÀ DEL RTI	RISULTATI / BENEFICI	CONDIVISIONE E RUOLI COINVOLTI
GOVERNO AQ	Indirizzo Strategico	Definizione strategia puntuale di gestione ed erogazione dei servizi	Principi guida condivisi / Unicità di approccio per le PA / Framework solido di gestione	Incontri trimestrali di RTI (RUAC, Board RTI, RT, EFPA)
	Allocazione Risorse	Gestione team ed allocazione risorse, staffing figure chiave per Governo ed Esecuzione	Staffing rapido e puntuale team di lavoro / Qualità delle risorse / Alta soddisfazione della PA	Staff Meeting Mensili (Resource & Knowledge Manager, RUAC, RT)
	Gestione della conoscenza & Best Practice	Diffusione della cultura della condivisione, gestione dell’informazione ed applicazione di best practices	Capitalizzazione know-how / Erogazione di best practice nella PA / Riuso e riutilizzo di soluzioni	Staff Meeting Mensili (Resource & Knowledge Manager, RUAC, RT)
	Gestione Piano Qualità Generale	Redazione e aggiornamento del Piano della Qualità Generale per l’Accordo Quadro	Conformità agli impegni / omogeneità dei servizi / standard di gestione della qualità	Condivisione trimestrale tramite Portale (RUAC, RT)
	Gestione Portale	Set up portale e collegamento con i sistemi dell’Amministrazione.	Punto unico di contatto e reporting	Set-up fornitura con manutenz. continua (RUAC, RT, TL)
	CONTRATTO ESECUTIVO	Piano Operativo & Orchestrazione Servizi	Definizione indirizzi specifici per erogazione servizi e set-up per deploy e identificazione di customizzazioni per le Amministrazioni	Framework standard per tutte le PA/Rapidità di predisposizione ed erogazione/Customizzazione servizi ad hoc
Presa in carico & Trasferimento Know-how		Redazione pian dettagliato con attività di presa in carico, impegno definito e strumenti per presa in carico e trasferimento finale	Piani coerenti e customizzati per le PA/ Rapidità di erogazione servizi / Linee guida omogenee	Awio & chiusura Contratto Esecutivo (RUAC CE, RT, RdS)
Gestione Piano Qualità Specifico CE		Redazione e aggiornamento del Piano della Qualità Specifico personalizzato per PA e caratteristiche funzionali/tecniche fabbisogno	Framework solido di riferimento / Presenza di check list standard	Awio Contratto Esecutivo (RUAC CE, RT, RdS)
Erogazione Servizi Oggetto della fornitura		Erogazione orchestrata dei servizi richiesti dall’Amministrazione in linea con l’AQ	Piani e progetti fabbisogni coerenti e customizzati per le PA/ Rapidità di erogazione servizi / Linee guida omogenee	Incontri periodici CE Mensili (RUAC CE, RT, TL, RdS, EFPA)
Monitoraggio KPI e rilievi fornitura		Valutazione continua stato fornitura e qualità erogazione in ottica <i>continuous improvement</i>	Qualità e omogeneità della fornitura , efficienza e concretezza dell’approccio adottato	Incontri periodici CE Mensili (RUAC CE, RT, TL, RdS, EFPA)

**PROCEDURE DI COORDINAMENTO:** Al fine di coordinare in modo efficiente ed efficace le attività ed indirizzare sin da subito le azioni del RTI verso un modello di funzionamento sinergico a beneficio delle Amministrazioni, è stato definito anche un apposito **framework di procedure di coordinamento**. Tali procedure contengono principalmente: le **regole per la gestione delle informazioni** nell'ambito del RTI, lo **scambio dei deliverable**, la gestione della qualità della fornitura ed i principali strumenti a supporto utilizzati. In particolare il RTI adotterà: una procedura di coordinamento di AQ – Master per l'AQ, contiene tutte le regole strategiche e di alto livello per la gestione complessiva dell'accordo quadro e rappresenta il "one source of truth" in relazione alla gestione dell'AQ grazie a tutte le informazioni in esso contenute; una procedura di coordinamento per ogni CE – Master per il CE, contiene le regole puntuali, customizzate a seconda dell'Amministrazione e del contesto del Fabbisogno oggetto del CE.

**PIANO DI PRESA IN CARICO:** La soluzione proposta per la gestione della presa in carico mette in campo consolidate esperienze delle aziende del RTI nel subentro in sistemi complessi nell'ambito della Pubblica Amministrazione e si basa principalmente sui due seguenti cardini: coinvolgimento del personale che verrà poi impegnato a regime nella fornitura, sia a livello di governo che di erogazione dei servizi e trasparenza sull'andamento del processo di subentro nei confronti di tutti gli attori interessati attraverso una governance operativa e focalizzata. In figura si riporta un esemplificativo del Piano di Presa in carico.

**Legenda:** Stipula Contratto ◆ Incontro/SAL ◆ Inizio Presa in Carico ◆ Fine presa in Carico/Inizio attività ◆

FASE	ATTIVITÀ	-W1	W1	W2	W3	W4
<b>Pianificazione</b>	Predisposizione Piano di Subentro	◆				
<b>Predisposizione Strumenti</b>	Predisposizione e aggiornamento strumenti		◆			
<b>Assessment documentale</b>	Analisi AS IS dei progetti in corso					
<b>Acquisizione competenze</b>	Incontri con il personale dell'Amministrazione e del fornitore uscente, training on the job, self training, workshop					
<b>Ottimizzazione</b>	Individuazione delle possibili aree di miglioramento					
<b>Fine presa in carico</b>	Ricognizione e verifica delle attività svolte					◆
<b>Governance</b>	Verifica dello stato delle attività	◆	◆	◆	◆	◆

**3.3 RUOLI, RISORSE E STRUTTURE AGGIUNTIVE PROPOSTI PER LA GESTIONE FORNITURA E MODALITÀ DI INTERAZIONE CON L'AMMINISTRAZIONE.** Al fine di realizzare in toto le sinergie proposte in organizzazione ed offrire i migliori servizi alle Amministrazioni, il RTI ha previsto l'integrazione del TL con i seguenti ruoli, risorse e strutture aggiuntive.

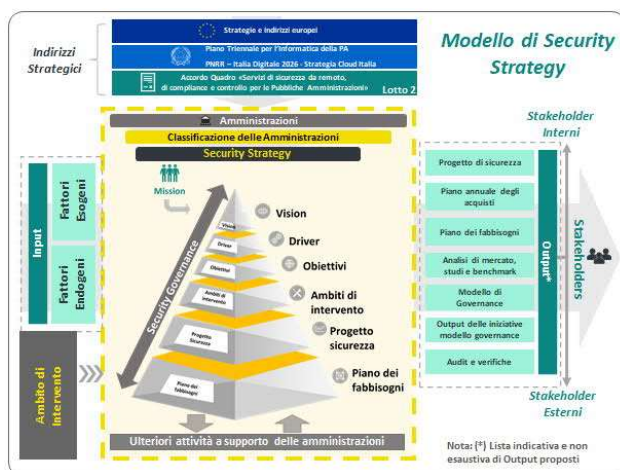
RUOLO	EFFICACIA	ADERENZA AL CONTESTO	COERENZA GENERALE	MOD. INTERAZIONE
<b>I&amp;D - Resp. Promozione AQ</b>	Garantisce un coordinamento unificato su promozione e comunicazione dell'AQ	Focalizzazione e specializzazione sulle caratteristiche dell'AQ	Punto unico per le attività di marketing e business development dell'AQ.	Workshop semestrali sui risultati dell'AQ
<b>I&amp;D - Resp. Finanz. e PNRR</b>	Assicura la valorizzazione dei progetti delle PA in termini di finanziabilità con fondi EU	Competenze cross-funzionali su tematiche funding e sui trend di sicurezza nella PA	Favorisce un incremento della capacità produttiva e di spesa delle PA in ambito sicurezza	Meeting trimestrale di condivisione delle opportunità PNRR
<b>I&amp;D - Innovation Leader</b>	Assicura il governo dell'innovazione e la sua introduzione nell'ecosistema delle PA	Expertise sui trend di cyber e di sicurezza più innovativi del mercato	Forte integrazione con i TL, grazie a modello di gestione interazioni definito	Workshop trimestrali sui trend di innovazione
<b>FdS - PMO AQ</b>	Garantisce la realizzazione di linee guida uniche e standard di erogazione	Conoscenza delle dinamiche di gestione degli AQ Consip	Elemento di coordinamento operativo delle attività di e monitoraggio delle erogazioni	Reportistica bimestrale sullo stato di avanzamento dell'AQ
<b>FdS - Resource Manager</b>	Gestione centralizzata che garantisce risposte efficaci ai picchi di lavoro	Dimensionamento efficiente dei TL in relazione ai fabbisogni delle PA	Sicurezza di presidio del processo di staffing	Reportistica bimestrale sullo staffing
<b>FdS - IQAM</b>	Garantisce omogeneità e standard elevati di qualità per i servizi della fornitura	Capacità di garantire i livelli qualitativi richiesti per forniture complesse in PA	Forte integrazione con i TL, grazie a modello di gestione interazioni definito	Report trimestrale checkpoint di qualità
<b>FdS - Knowledge Manager</b>	Assicura il costante allineamento delle skill delle risorse rispetto agli standard del mercato	Capacità di garantire il livello di aggiornamento necessario per la PA	Forte integrazione con i TL, grazie a modello di gestione interazioni definito	Reportistica bimestrale sulla formazione delle risorse
<b>EFPA</b>	Guida le PA nelle sfide del settore, per una transizione digitale sicura	Profonda conoscenza dei processi e delle tematiche tipiche delle PA	Indirizza le attività delle strutture dell'organizzazione in base delle esigenze della PA	Workshop trimestrali sui trend della PA digitale
<b>RdS</b>	Garantiscono omogeneità di erogazione e capacità di customizzazione delle soluzioni	Know-how specialistico settore Cyber security	Indirizza le attività dei TL sulla base delle caratteristiche dei servizi	Meeting trimestrali di condivisione Best practices

#### 4 PROPOSTA PROGETTUALE PER IL SERVIZIO "SECURITY STRATEGY"

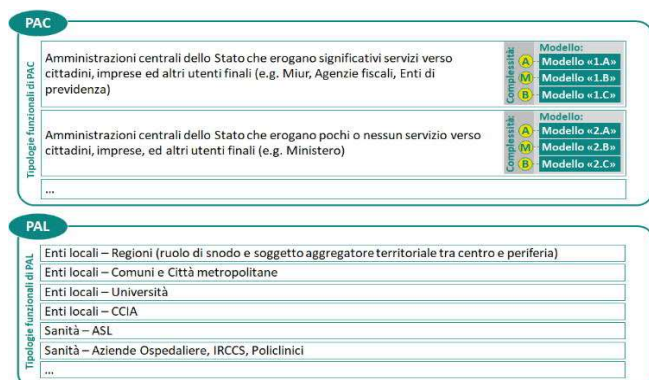
La strategia di sicurezza è l'abilitatore fondamentale che consente di individuare le azioni più appropriate per gestire i rischi di sicurezza in coerenza con le specificità delle Amministrazioni individuando le modalità con cui raggiungere i livelli di sicurezza richiesti e al contempo assicurare la conformità alle normative vigenti ed alle direttive di settore. La proposta del RTI è caratterizzata dai seguenti elementi distintivi.

1. Approccio concreto di elaborazione del **Progetto di Sicurezza** (di seguito **PdS**) tramite **modelli di PdS** differenziati sulla base della classificazione e della complessità delle Amministrazioni (**MappaPA**). 2. Disponibilità di **benchmark della maturità e dello spending di mercato in ambito Sicurezza ICT** acquisiti collezionando i dati provenienti da **migliaia di valutazioni effettuate ogni anno nel mondo**, ottenendo una vista **privilegiata** e completa in termini di **andamento** del settore su base **nazionale e internazionale**. Tale patrimonio sarà utilizzato come strumento di supporto nell'elaborazione del PdS. 3. In aggiunta, il RTI è disponibile a **collezionare e confrontare i valori economici** medi dei servizi acquisiti dal Lotto 1, al fine di fornire a Consip ed alle Amministrazioni uno strumento utile a **verificare coerenza/omogeneità dei servizi acquisiti** rispetto alle necessità identificate nei PdS.

**4.1 PROPOSTA DI ELABORAZIONE DEL PROGETTO DI SICUREZZA E MODELLO CORRELAZIONE DEI SERVIZI. 4.1.1 PROGETTO DI SICUREZZA.** Il RTI si impegna ad erogare le attività in ambito nel rispetto dei requisiti tecnico-funzionali specificati nel CTS. Allo scopo di supportare le Amministrazioni nella pianificazione strategica della Sicurezza ICT, il RTI prevede l'utilizzo di uno specifico **Modello di Security Strategy**, sviluppato sulla base di standard e leading practices riconosciute in ambito Security ICT (es. ISO27001-2, ISO27017-8, ISO27701 ISO31000, ISA62443, NIST800.53 v5, Framework Nazionale, Linee guida ENISA). Tramite tale modello l'Amministrazione sarà in grado di recepire gli indirizzi strategici (a livello nazionale ed europeo) e gli input esogeni ed endogeni, per definire - attraverso l'ausilio di metodologie, approcci operativi e strumenti - il PdS. Il PdS, coerentemente con il contesto di riferimento e con le esigenze di stakeholder interni ed esterni, avrà lo scopo di attuare la Missione e la derivata Visione dell'Amministrazione (i.e. la trasposizione della Missione in una strategia a lungo termine di evoluzione tecnologica e/o organizzativa mirata al suo soddisfacimento). Con riferimento agli ambiti del PdS, allo scopo di articolare una risposta completa rispetto a tutte le fasi del ciclo di vita della sicurezza delle informazioni e dei sistemi ICT, il RTI propone di considerare, a titolo indicativo e non esaustivo, i seguenti **Ambiti di intervento**: **Identify**: strategia e pianificazione, Governance Asset e Processi, gestione del rischio cyber, security assurance (VA, PT, Testing del Codice), sicurezza terze parti e contratti di servizio, Compliance normativa **Protect (Management)**: Information & Data Security, Identity & Access Management, Security by Design e Secure SDLC, Application & System Protection, Network Protection, Data Center Security, Secure



Cloud Computing, Cyber Awareness & Training, Security Operations •**Detect**: Monitoraggio continuo di sicurezza, Incident Detection, Threat intelligence, Threat Hunting; •**Response**: Cyber Incident Response, Investigation and Forensics •**Recovery**: Continuità Operativa and Crisis Management, Disaster Recovery. Il valore aggiunto apportato dal RTI è l'adozione di un **approccio flessibile** in grado di supportare le Amministrazioni nella elaborazione di **PdS concreti, efficaci e sostenibili**, che si adatterà alla tipologia, al livello di complessità ed alle esigenze di protezione dell'amministrazione. A tal fine, il RTI ha sviluppato un **metodo di classificazione delle Amministrazioni** basato sulle **tipologie funzionali** integrate da una dimensione di **complessità**, **quest'ultima** basata su: •numerosità dei servizi offerti a cittadini, imprese o altri utenti •dimensione dell'amministrazione (es. dimensioni dei Comuni) •criticità dei dati degli utenti trattati (es. Enti Sanitari vs Università) •livello di centralità in relazione a tematiche di cooperazione ed interconnessione con le altre Amministrazioni •contesto normativo applicabile. Sulla base di tale metodo e delle esperienze consolidate in ambito Sicurezza ICT, trasversalmente ad entrambi le classi delle



PA, il RTI intende proporre l'utilizzo di specifici **modelli (prototipi) di PdS**, in termini di obiettivi ed ambiti da indirizzare, sulla base dei **profili di rischio** associati alle differenti combinazioni di Tipologia e Complessità. **(fase 1)** Il prototipo è uno strumento, differenziato in funzione delle dimensioni sopra considerate, finalizzato ad una rapida ricognizione dei presidi di sicurezza esistenti integrando, laddove disponibili, gli esiti del questionario di autovalutazione del livello di applicazione dei controlli ABSC delle misure minime di sicurezza AGID. **(fase 2)** Tale ricognizione includerà una serie di fattori determinanti per la definizione di un Progetto efficace e concreto, in particolare: •le iniziative in essere e previste in materia di sicurezza informatica e sicurezza delle informazioni •il modello IT, gli elementi infrastrutturali, organizzativi, applicativi esistenti e di prossima introduzione (es. PSN, evoluzione verso architetture

cloud) •Regolamenti e disposizioni organizzative interne •specifiche minacce cyber applicabili al contesto e relativi rischi, inclusi quelli legati alla gestione dei contratti di servizio •risk appetite, in relazione al profilo di rischio dell'Amministrazione •ulteriori elementi, ove disponibili, quali ad esempio risultati di audit, assessment, incidenti di sicurezza. Tale approccio rappresenta un elemento preliminare e facilitatore nel disegno dei Progetti delle singole Amministrazioni e sarà personalizzato sulla base del contesto ed in particolare del livello di digitalizzazione dell'Amministrazione stessa. Nel caso **delle Amministrazioni meno complesse**, tipicamente contraddistinte da minore strutturazione dei presidi di sicurezza e limitate capacità di investimento, il valore aggiunto di questo approccio è **quello di rendere accessibile lo strumento di pianificazione della sicurezza ICT (PdS)**, grazie ad un minor effort richiesto, alle Amministrazioni stesse nella definizione degli obiettivi e degli ambiti del Progetto. Il RTI dispone dei modelli di base coerenti con le principali tipologie funzionali di Pubblica Amministrazione, con ulteriori declinazioni relative a settori specifici ed a maggiore criticità (es. il modello sviluppato per l'ambito specifico degli Enti ospedalieri). Partendo dai modelli di base, durante lo svolgimento delle attività progettuali saranno adattati/sviluppati ulteriori modelli specifici per meglio cogliere le peculiarità di ogni tipologia di amministrazione, favorendo la **logica del riuso e l'ottimizzazione conseguente dei costi**. Allo scopo di incrementare la consapevolezza delle Amministrazioni, i modelli proposti dal RTI saranno pubblicati nell'“Area Informativa” del Portale, riservata alle Amministrazioni. Sulla base delle informazioni raccolte e del Modello di Security Strategy, l'elaborazione del PdS si concretizzerà in un percorso analitico che a partire dalla **Missione** dell'Amministrazione, **(fase 3)** definirà la **Visione** strategica di sicurezza e i relativi driver. Tali driver saranno declinati **(fase 4)** in **Obiettivi** strategici, tattici e operativi, per il cui raggiungimento saranno definite **(fase 5)** specifiche iniziative correlate agli **ambiti di intervento** del PdS dell'Amministrazione. **4.1.1.1**

**SUPPORTO ALLA GOVERNANCE E ULTERIORI ATTIVITÀ. Supporto alla Governance** Funzionalmente a quanto sopra, il Modello proposto dal RTI prevede il disegno e la realizzazione di una Security Governance dinamica il cui valore aggiunto è quello di: •garantire il controllo di quanto indirizzato a livello strategico •rivalutare il PdS sulla base dei risultati ottenuti e/o delle nuove esigenze di Sicurezza ICT derivanti da eventuali evoluzioni delle normative, delle architetture, delle tecnologie e del modello IT dell'Amministrazione. Con riferimento al **disegno del modello di governance**, il RTI supporterà le Amministrazioni nella •**(Fase 1)** formulazione di una strategia e di una architettura di monitoraggio del contesto interno ed esterno •**(Fase 2)** definizione di una dashboard di monitoraggio del PdS dell'Amministrazione che individui e rappresenti KPI, KRI e metriche di sicurezza (*Cyber Security Dashboard*). La **declinazione operativa della governance** includerà quindi le seguenti attività: •**Monitoraggio**: attività di verifica dell'andamento del PdS delle Amministrazioni tramite attività di reporting, analisi dei risultati, tracciatura e supporto nella gestione di eventuali problematiche di progetto •**Controllo**: attività utili a verificare la coerenza delle iniziative del PdS rispetto alle scelte strategiche •**Gestione del rischio**: attività volte a valutare (anche nel continuo attraverso l'utilizzo di KRI) e gestire il livello di esposizione al rischio di sicurezza garantendo il rispetto dei livelli di rischio di sicurezza ICT all'interno di soglie di tolleranza definite •**Gestione delle classificazioni e tassonomie**: attività volte ad assicurare uniformità di classificazioni e tassonomie nei processi di sicurezza •**Lesson learned**: attività di rielaborazione delle indicazioni strategiche funzionalmente ai dati provenienti dai singoli servizi •**Gestione delle risorse**: attività volte ad assicurare, un utilizzo efficiente di tutte le risorse economiche e tecniche nell'ambito del PdS dell'Amministrazione in linea con quanto previsto nei fabbisogni. **Ulteriori Attività a Supporto**. Il RTI fornirà inoltre ulteriori attività di supporto consulenziale in ambito Sicurezza ICT a favore dell'Amministrazione, trasversalmente alle attività precedenti, il cui valore aggiunto è rappresentato dall'utilizzo delle migliori capacità ed esperienze similari nella definizione, coordinamento e monitoraggio di PdS, quali ad esempio: •**Predisposizione analisi, studi e benchmark** in materia di sicurezza informatica volti a supportare le scelte di modello IT e di sicurezza dell'Amministrazione in coerenza con il processo di trasformazione digitale (nuova architetture on-premise, cloud, ibrido, PSN, etc.) •**Consulenza tecnico-specialistica** di supporto agli stakeholder delle strutture di vertice ICT dell'Amministrazione con particolare riferimento alle valutazioni e processi decisionali •**Promozione, affiancamento e partecipazione** a gruppi di lavoro, comitati, tavoli di coordinamento, per mettere a fattor comune elementi utili ai PdS delle singole Amministrazioni, la definizione delle strategie, l'analisi delle esigenze, la produzione di documentazione (es. politiche, linee guida) •**Interfaccia con i provider tecnologici** con l'obiettivo di analizzare e indirizzare eventuali elementi di natura tecnologica, garantendo un efficace allineamento al PdS.

**4.1.2 MODELLO CORRELAZIONE SERVIZI.** Il PdS potrà inoltre beneficiare di una correlazione tra i servizi del Lotto 2 nonché del Lotto 1 e/o di altre iniziative in essere, secondo una proposta di interdipendenza tra gli stessi servizi. Tale approccio consentirà di realizzare un ciclo di gestione completa della sicurezza (Plan,



Do, Check, Act): ● pianificando le azioni strategiche da attivare in funzione dei risultati attesi dalle singole iniziative e in coerenza con le linee strategiche (Plan, Do) ● prioritizzando l'esecuzione dei servizi di controllo (in termini di perimetro, tipologia, ecc.) in coerenza con le linee strategiche stesse, misurando l'efficacia degli interventi realizzati (Check) ● aggiornando la pianificazione delle azioni da svolgere in funzione delle risultanze integrate dei servizi testing (Act). A tale scopo il RTI ha elaborato il **Modello Correlazione Servizi** esemplificativo delle principali correlazioni, evidenziando le principali fasi del ciclo di vita dei servizi del Lotto 2, dalla

strategia, attraverso le verifiche tecniche e di compliance fino alla risposta in termini di analisi, progettazione e verifica dei processi di gestione incidenti.

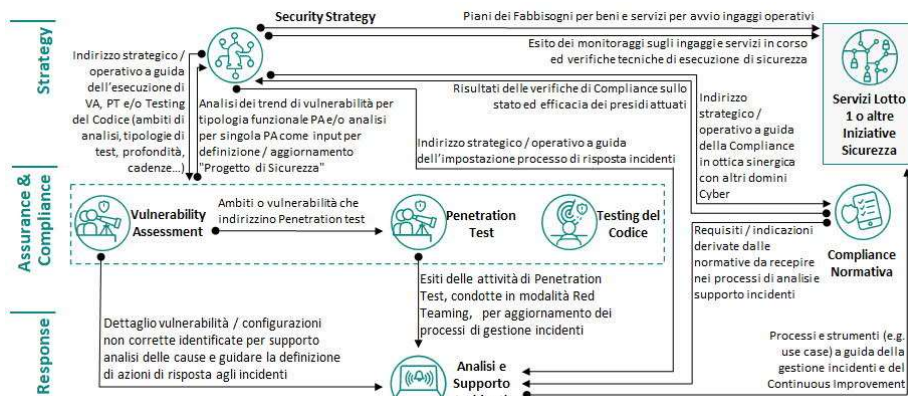
**4.1.3 DELIVERABLE.** Sono previsti i seguenti deliverable, salvo ulteriori concordati con le Amministrazioni.

Deliverable	Contenuti esemplificativi
PdS	Documento unitario e integrato contenente la descrizione dell'insieme delle iniziative di sicurezza, nello specifico, a titolo esemplificativo e non esaustivo: ● Analisi del contesto e individuazione delle macro esigenze; ● Vision e obiettivi strategici, tattici e operativi; ● Definizione degli ambiti di intervento e dettaglio delle relative iniziative di sicurezza in termini di attività previste e approccio operativo, risultati attesi, roadmap di implementazione e stime dei costi di realizzazione. Il documento potrà avere viste differenti in funzione dei differenti interlocutori (es. DG, ICT). Modello di governance e i relativi processi a supporto degli indirizzi strategici di sicurezza e del relativo progetto
Report delle verifiche	I report includono le evidenze delle verifiche ● tecnico-economiche sui servizi erogati tramite Lotto 1 e/o altre iniziative in essere ● indicazioni delle potenziali anomalie/non conformità e azioni di remediation ● completezza del documento di Contesto Tecnologico ed Applicativo ● elementi costitutivi e raggiungimento dei risultati attesi dei servizi erogati dai fornitori del Lotto 1.

**4.1.4 STRUMENTI E SOLUZIONI TECNOLOGICHE.** Di seguito sono riportati i principali strumenti/soluzioni tecnologiche che saranno utilizzati per l'erogazione del servizio. Gli strumenti/tool di analisi riportati di seguito sono da intendersi a titolo non esaustivo. Nel corso delle attività, anche in considerazione dell'evoluzione delle minacce cyber, dell'utilizzo di tecnologie specifiche da parte dell'Amministrazione nonché dell'evoluzione del processo tecnologico potranno essere utilizzati ulteriori strumenti al fine di garantire un livello di qualità elevato nel corso delle attività.

Ambito di utilizzo	Principali strumenti
Supporto all'elaborazione del PdS	<b>CSF – Cyber Strategy Framework</b> - strumento <b>proprietario</b> web-based che, sulla base della Mission dell'Amministrazione, supporta la definizione della Vision strategica di cybersecurity. Basandosi su attività di benchmark, alimentate da una banca dati di clienti esistenti coerenti con il perimetro di gara, lo strumento facilita la definizione del "target state" in termini di postura cibernetica, e consente di monitorarne l'incremento di maturità nel tempo.
	<b>IBA – Industry Benchmark Analytics</b> – strumento <b>proprietario</b> che, consolidando i dati e risultati delle attività in ambito (Lotto 1/2), e/o provenienti dai dati di benchmark collezionati dal RTI, avvalendosi dell'ecosistema interno ed esterno per l'Innovazione, formulerà una banca dati nazionale, utile a supportare la produzione di studi e analisi. Questi studi saranno poi utilizzati come elemento di paragone per aggiungere ulteriore valore all'erogazione dei servizi.
	<b>GISS – Global Information Security Survey</b> – Rilevazione periodica che da oltre 20 anni esplora il panorama globale dell'information security in termini di trend, spending e utilizzo tecnologie innovative. La base dati dello strumento fornisce in particolare viste per tutti i settori aziendali e per la Pubblica Amministrazione in particolare.
Supporto alla Security Governance	<b>CPA – Cyber Program Assessment</b> - strumento <b>proprietario</b> web-based che ingegnerizza e permette di eseguire attività di security assessment a 360° comprensive di aspetti organizzativi, processi, e tecnologici basate su standard riconosciuti (ISO 27001, NIST, Framework Nazionale per la Cyber Security e la Data Protection) che possano supportare la definizione e realizzazione del PdS. Lo strumento si basa su attività di benchmark utili per l'analisi della maturità cibernetica dell'Amministrazione.
	<b>CRM – Cyber Risk Management</b> - strumento <b>proprietario</b> a supporto delle attività di contestualizzazione, identificazione, analisi, trattamento, monitoraggio e reportistica del rischio cibernetico. Include Risk Appetite Framework (RAF) e il modello dei KRI.
	<b>TPRM – Third Party Risk Management</b> - strumento <b>proprietario</b> web-based per la gestione della sicurezza delle terze parti a supporto della valutazione del rischio legato ai contratti di fornitura dei servizi erogati.
	<b>CSD – Cyber Security Dashboard</b> - strumento <b>proprietario</b> web-based per il reporting operativo e direzionale, che sulla base degli input raccolti dalle iniziative di sicurezza (es. monitoraggio sugli incidenti di sicurezza o vulnerabilità emerse), consente di correlare le informazioni, e monitorarne l'andamento attraverso l'analisi di specifici KPI. -

**4.2 PROPOSTA DI ELABORAZIONE DI UN MODELLO DI ANALISI DEI FABBISOGNI DI BENI E SERVIZI DI SICUREZZA.** Il RTI propone, tenuto conto di contesto e peculiarità dell'Amministrazione, mutuando l'approccio seguito per la determinazione dei modelli di PdS, l'identificazione di **modelli (prototipi) di piano di fabbisogni** in base alle differenti combinazioni di Tipologia e Complessità delle Amministrazioni, al fine di indirizzare una corretta gestione delle necessità di beni e servizi dalla caratterizzazione dell'esigenza alla redazione del Piano del fabbisogno. A partire dall'identificazione del fabbisogno originato da una esigenza emersa da una iniziativa del Piano strategico, dagli studi e analisi di mercato, da spunti forniti dal RTI grazie all'ecosistema di innovazione proposto o da eventi



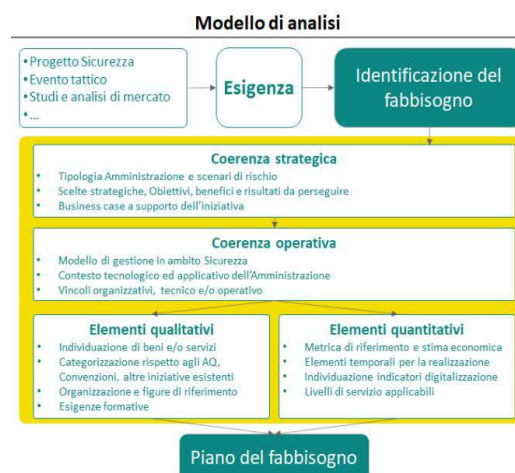
operativi occorsi (ad esempio un incidente, una vulnerabilità), il modello proposto analizzerà le informazioni da prevedere all'interno del Piano del fabbisogno e si compone dei macro-ambiti:

● **(Fase 1) Coerenza strategica:** sulla base di obiettivi ed ambiti previsti nel PdS (§3.1.1.1), saranno valutati gli obiettivi, i benefici ed i risultati da perseguire tramite la fornitura allo scopo di garantirne il necessario allineamento con le linee strategiche dell'Amministrazione; laddove richiesto, il RTI fornirà supporto anche alla redazione di un business case della fornitura per facilitare il processo di richiesta del budget necessario.

● **(Fase 2) Coerenza operativa:** tali analisi saranno necessarie per garantire l'integrazione dei beni e dei servizi oggetto della fornitura nel modello esistente di gestione sia IT sia Sicurezza; saranno in particolare valutati il contesto tecnologico ed applicativo esistente nonché eventuali vincoli organizzativi, tecnico e/o operativo che potrebbero avere un impatto sull'adozione dei beni e/o l'erogazione dei servizi oggetto della fornitura.

● **(Fase 3) Elementi qualitativi:** tale analisi fornirà una caratterizzazione completa dei beni e servizi allo scopo di categorizzarli e prevede un supporto da parte del RTI nell'individuazione degli AQ, delle Convenzioni e di altre iniziative esistenti di cui l'Amministrazione vorrà usufruire; saranno contestualmente valutate la struttura organizzativa e le figure di riferimento (sia Amministrazione sia Fornitore) da prevedere nella fornitura nonché le eventuali esigenze formative correlate con la realizzazione dell'intervento.

● **(Fase 4) Elementi quantitativi:** in tale ambito, il RTI supporterà la definizione delle metriche di riferimento (es. giorni/persona del team ottimale) e della stima economica attesa nonché dei tempi di attivazione ed esecuzione della fornitura, esplicitando le principali milestone attese dall'Amministrazione; saranno inoltre individuati gli indicatori di digitalizzazione da prevedere ed i livelli di servizio previsti dagli AQ, convenzioni o altre iniziative individuate nell'ambito qualitativo. Con riferimento all'attività di analisi delle stime quantitative ed economiche dei servizi previsti nell'ambito del Lotto 1, il RTI propone, quale elemento migliorativo utile ad abilitare quel controllo imparziale dei servizi di sicurezza del Lotto 1 dichiarato come obiettivo del Lotto 2, di realizzare un **benchmark continuamente aggiornato utile a confrontare i valori economici medi dei servizi acquisiti dal Lotto 1**. Quale ulteriore elemento di valore aggiunto e con riferimento alle ulteriori attività richieste in tale ambito, il RTI metterà a disposizione la sua profonda esperienza in ambito di Program e Project Management di iniziative di Sicurezza ICT complesse, applicando l'architettura di monitoraggio definita (§4.1.1.2) per il controllo ed il coordinamento dei piani di attuazione dei servizi di sicurezza erogati da remoto a favore dell'Amministrazione, anche al fine di verificare il raggiungimento dei risultati attesi. Il RTI fornirà inoltre supporto all'elaborazione del piano annuale degli acquisti in materia di sicurezza ICT dell'Amministrazione.



**4.2.1 DELIVERABLE.** Sono previsti i seguenti deliverable, salvo ulteriori concordati con le Amministrazioni nell'ambito dei CE

Deliverable	Contenuti esemplificativi
Piano annuale degli acquisti	Piano di investimento annuale a supporto delle iniziative di sicurezza identificate nel PdS.
Analisi di mercato, studi e benchmark	Documenti relativi ad analisi di mercato, studi e benchmark effettuati dal RTI sulla base di esperienze correnti e pregresse che supporteranno le attività previste nell'ambito del servizio di Security Strategy tra cui a titolo esemplificativo e non esaustivo: ● definizione dei fabbisogni; ● analisi della postura cibernetica dell'Amministrazione ● definizione del "target state" dell'Amministrazione, ● definizione della Vision strategica dell'Amministrazione, ● stime quantitative e qualitative, etc.
Piano dei fabbisogni	Documento contenente le esigenze di approvvigionamento dell'Amministrazione legate alle iniziative identificate nel PdS, in termini di: ● indicazione delle macro-esigenze in linea con il PdS; ● descrizione delle iniziative previste; ● caratteristiche tecniche del servizio (es. team coinvolto, attività on site o da remoto); ● modalità e tempi di realizzazione. Il documento conterrà inoltre una scheda di sintesi per ogni iniziativa con indicazione delle fasi progettuali (es. avvio, erogazione, chiusura) e dell'effort previsto per ciascuna di esse.

**4.2.2 STRUMENTI E SOLUZIONI TECNOLOGICHE.** Di seguito sono riportati i principali strumenti/soluzioni tecnologiche che saranno utilizzati per l'erogazione del servizio. Gli strumenti/tool di analisi riportati di seguito sono da intendersi a titolo non esaustivo. Nel corso delle attività, anche in considerazione dell'evoluzione delle minacce cyber, dell'utilizzo di tecnologie specifiche da parte dell'Amministrazione nonché dell'evoluzione del processo tecnologico potranno essere utilizzati ulteriori strumenti al fine di garantire un livello di qualità elevato nel corso delle attività.

Principali strumenti
<b>IBA – Industry Benchmark Analytics</b> – strumento <b>proprietario</b> che, consolidando i dati e risultati delle attività in ambito (Lotto 1/2), e/o provenienti dai dati di benchmark collezionati dal RTI, avvalendosi dell'ecosistema interno ed esterno per l'Innovazione, formulerà una banca dati nazionale, utile a supportare la produzione di studi e analisi. Questi studi saranno poi utilizzati come elemento di paragone per aggiungere ulteriore valore all'erogazione dei servizi.

**4.3 TEAM DI LAVORO.** Il team ottimale rispetterà i requisiti specificati nel CTS a cui si aggiungeranno i requisiti migliorativi sintetizzati di seguito.

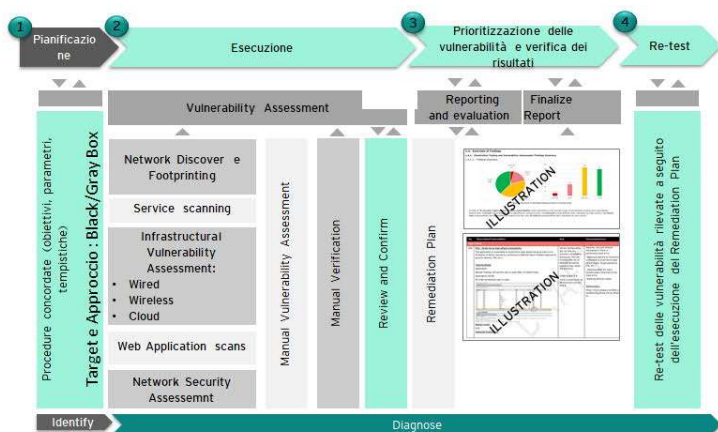
Profilo	Requisito migliorativo Generale	Requisito migliorativo Specifico
Security Principal	Nel team sarà inclusa almeno una risorsa con attestato <b>ITIL Foundation v3/v4 o Prince 2 Foundation/IPMA/PMI</b>	
Security Solution Architect		
Senior Information Security Consultant		Possesso della qualifica di <b>Lead Auditor ISO 27001</b> aggiornata all'ultima release, per <b>almeno il 70%</b> delle risorse, appartenenti al suddetto profilo professionale, nell'ambito di ciascun contratto esecutivo
Senior Security Auditor		
Data Protection Specialist		

## 5 PROPOSTA PROGETTUALE PER IL SERVIZIO "VULNERABILITY ASSESSMENT"

Il servizio di Vulnerability Assessment prevede l'identificazione in maniera proattiva, mediante una verifica dinamica della sicurezza, delle vulnerabilità presenti su dispositivi di rete, software e applicazioni delle Amministrazioni e la mitigazione dei rischi cyber connessi. Il RTI si impegna ad erogare le attività in ambito al presente servizio nel rispetto dei requisiti tecnico-funzionali specificati nel CTS, facendo affidamento sugli elementi distintivi sotto riportati.

**1. Standardizzazione del reporting** e dei piani di prioritizzazione/remediation attraverso l'utilizzo di una **piattaforma centralizzata** (denominata Bug Blast) ed **indipendente dai motori di scansione** (vulnerability scanner), garantendo ripetibilità ed uniformità dei risultati **2. Metodologia per la definizione del "remediation plan" con approccio risk-based** e reportistica in grado di rappresentare le vulnerabilità identificate sia ad interlocutori executive che tecnici, fornendo pratici strumenti operativi per agevolare la risoluzione delle stesse **3. Centri di eccellenza nazionali ed internazionali in ambito Cybersecurity** (Roma, Milano, Bari, ed oltre 10 in EU), con la presenza di **laboratori specialistici** e con professionalità verticali su attività di Offensive Security. Tali centri supportano i team nella raccolta di informazioni relative a nuove vulnerabilità (es. mediante tecniche di Cyber Threat Intelligence) e tecniche innovative per lo sfruttamento delle stesse **4. Eterogeneità nella copertura degli ambienti target (IT/OT/IoT/Cloud)** attraverso strumenti e tecniche idonee e specifiche a garantire il discovery per ciascuna tipologia di target **5. Ampio supporto nel discovery di misconfiguration e vulnerability specifiche per gli ambienti di cloud computing** (IaaS, PaaS, SaaS), anche in presenza di CSP differenti (AWS, Azure, Google, ecc.).

**5.1 MODALITA' DI ESECUZIONE DEL SERVIZIO.** Le attività di Vulnerability Assessment (VA) forniranno evidenze di dettaglio sulle vulnerabilità riconducibili



all'infrastruttura ICT e IoT/OT (es. dispositivi interconnessi impiegati nei diversi contesti di utilizzo - es. smart city, ambito sanitario, progetti open data), funzionali anche ad elaborare una *baseline* iniziale del livello di vulnerabilità e di esposizione del sistema informativo dell'Amministrazione. L'attività sarà svolta sia con strumenti automatici (continuamente aggiornati rispetto alle vulnerabilità di nuova identificazione) sia con strumenti definiti ad-hoc (es. script) sulla base della tipologia del target oggetto di analisi. Le attività saranno inoltre supportate dall'ecosistema di innovazione interno ed esterno (§ 14). Il RTI, sulla base della propria esperienza e del contesto di riferimento in cui saranno svolte le analisi di sicurezza, proporrà gli strumenti di analisi più adatti per l'esecuzione dei VA (open-source, proprietari e/o di mercato). Le attività di VA eseguite sono basate sulle metodologie OSSTMM, OWASP, PTES, NIST

800-52/53 e ISA 62443, riconosciute globalmente come standard de-facto. L'applicazione di tali metodologie garantirà risultati coerenti, ripetibili e misurabili. Nell'ambito delle attività di VA terremo in considerazione il sempre più diffuso utilizzo delle tecnologie Cloud da parte delle Amministrazioni, in coerenza con quanto definito dalla Strategia Cloud Italia. A tal fine, su specifica richiesta dell'Amministrazione, il RTI è in grado di integrare all'interno dei servizi offerti anche l'esecuzione di attività di Assessment del livello di sicurezza dei servizi Cloud IaaS e SaaS, verificandone la compliance rispetto a standard, requisiti normativi e best practice di settore, e ricercando vulnerabilità celate negli errori di configurazione dei diversi ambienti cloud. Il RTI potrà eseguire le attività di VA in maniera periodica ove richiesto e ritenuto opportuno. Le attività saranno eseguite in modalità **Black-box**, che presuppone la verifica del livello di sicurezza dei target senza alcuna credenziale di accesso (non autenticato), e **Gray-box**, ovvero verifica del livello di sicurezza dei target simulando un attaccante che possiede una parziale conoscenza dell'infrastruttura oggetto di analisi e credenziali di accesso con privilegi base (autenticato). Per l'esecuzione dei servizi richiesti dall'Amministrazione, la metodologia prevede l'esecuzione di **4 fasi progettuali**: *Pianificazione delle attività, Esecuzione dei Vulnerability Assessment, Prioritizzazione delle vulnerabilità e verifica dei risultati, Re-test delle vulnerabilità a seguito del remediation plan*. Il RTI propone l'adozione di una piattaforma specifica per l'esecuzione di attività di Vulnerability Assessment. La **Piattaforma Bug Blast** ha l'obiettivo di fornire **report personalizzati e di tracciare le vulnerabilità dalla fase di discovery e per tutte le fasi di remediation**, offrendo sempre un **approccio agnostico rispetto ai vendor** utilizzati per la scansione. Le informazioni che afferiscono alle attività di VA richieste saranno disponibili nel portale tramite un sistema di autorizzazione granulare e le Amministrazioni potrà accedere a tali informazioni sulla base del periodo di retention che sarà concordato di volta in volta con le stesse e comunque, salvo diversa indicazione da parte dell'Amministrazione e nel rispetto delle normative vigenti, per un periodo garantito non inferiore a 1 mese dalla fine delle attività. Tale modalità di erogazione è consigliata dal RTI, che tuttavia è disponibile ad adattare la stessa sulla base di eventuali esigenze delle Amministrazioni, concordandole di volta in volta con le stesse. **Approccio operativo.** L'approccio operativo proposto dal RTI prevede l'esecuzione di tutte le attività tecniche previste dal CTS. Si sottolinea che quanto riportato di seguito offre una vista di alto livello delle attività operative che saranno svolte dal team: **•Pianificazione**: tale fase è fondamentale per la pianificazione delle attività di VA (tempi e orari) e per la raccolta delle informazioni necessarie all'esecuzione di verifiche di sicurezza efficaci. Nello specifico saranno eseguite le seguenti macro-attività: **▪ Identificazione degli stakeholder rilevanti** **▪ Richiesta e raccolta della documentazione in ambito** (es. disegni di rete, analisi funzionale, requisiti di sicurezza), nonché delle informazioni preliminari all'esecuzione dei VA (es. URL, indirizzi IP); **▪ informazioni necessarie per identificare le normative applicabili** (es. GDPR) e degli standard di sicurezza applicati dal cloud provider (es. ISO27001), **▪ Condivisione con l'Amministrazione delle metodologie, degli strumenti e delle modalità di esecuzione.** La proposta di modalità di scansione sarà condivisa con l'Amministrazione in base a: **criticità target, rilevanza dei target in ambito GDPR, potenziali impatti su sistemi legacy, bottleneck su alcuni sistemi/segmenti di rete, ecc.** **▪ Definizione del piano di dettaglio delle attività, comprensivo di data di inizio, fine e orari di esecuzione, per definire le migliori finestre temporali per minimizzare i rischi connessi all'interruzione del servizio e/o al degrado delle performance** **▪ Comunicazione all'Amministrazione degli IP delle macchine che eseguiranno i VA** **▪ Esecuzione di test di raggiungibilità/accesso del target oggetto di analisi** **▪ Richiesta di autorizzazione per l'avvio delle attività** **•Esecuzione**: in tale fase sono rilevate le vulnerabilità presenti per i target oggetto di analisi mediante tool automatizzati e tecniche manuali. I tool di analisi utilizzati per l'esecuzione delle scansioni automatizzate saranno opportunamente scelti e configurati (es. policy di scansione, credenziali di accesso ai tenant cloud) coerentemente con il contesto



specifico dei target. I relativi risultati saranno analizzati e correlati dal Team operativo. Nello specifico nella fase di Esecuzione sono eseguite le seguenti macro-attività: • **Discovery**: censimento e mappatura dei dispositivi presenti nel segmento di rete designato, identificazione del sistema operativo, dei servizi attivi e la loro relativa versione mediante attività di *Banner Grabbing e Fingerprint*, identificazione degli indirizzi associati ai target oggetto di analisi e identificazione delle informazioni tecniche in caso di analisi delle reti WiFi (es. SSID) • **Assessment**: scanning automatizzato dei target in ambito per la rilevazione delle principali vulnerabilità esistenti. Per quanto concerne le reti WiFi è effettuata una verifica della tipologia di autenticazione e la tipologia di protocolli di sicurezza implementati (WEP, WPA, WPA2, WPA Enterprise). Nel corso della fase di VA, inoltre, sono effettuate verifiche volte a rilevare la mancanza o non corretta implementazione di tecnologie di prevenzione, riconoscimento e risposta a possibili attacchi (IDS/IPS, log monitoring, ecc.). Ove possibile, per le vulnerabilità rilevate sarà effettuata una verifica manuale al fine di identificare ed eliminare i falsi positivi; tale attività è svolta mediante processi innovativi di controllo, sviluppati nel corso delle esperienze in ambito Offensive Security e tramite il supporto dei Centri di eccellenza del RTI, che consentono di ridurre al minimo la presenza di errori. La modalità si presta anche all'esecuzione di campagne periodiche o ricorrenti sulla base delle effettive esigenze espresse dall'Amministrazione • **Prioritizzazione delle vulnerabilità e verifica dei risultati**: le vulnerabilità identificate dagli strumenti di analisi saranno classificate (grazie alle opportunamente configurazioni preliminari) inizialmente dagli stessi in maniera automatica in base al sistema di **scoring CVSS**. Successivamente saranno **riviste in maniera critica dagli analisti per escludere i falsi positivi** e fornire una **migliore contestualizzazione** per l'Amministrazione, correlando ulteriori elementi quali: impatto del target (ACR - Asset Criticality Rating), impatto rispetto al GDPR, severità della vulnerabilità, complessità nello sfruttamento, livello di diffusione delle minacce derivate da attività di Cyber Threat Intelligence (VPR - Vulnerability Priority Rating) • **Predisposizione Remediation Plan**: Per ogni vulnerabilità identificata saranno fornite raccomandazioni sulle azioni da intraprendere per la loro risoluzione o mitigazione con anche indicazione delle priorità sempre in coerenza con le policy dell'Amministrazione e il livello di criticità/rischio precedentemente determinato. Queste saranno riportate all'interno di un piano di rientro concreto e applicabile al contesto (con indicazione anche delle tempistiche di risoluzione condivise con l'Amministrazione) in grado di supportare le linee tecniche dell'Amministrazione nella risoluzione. I risultati delle attività di VA e le raccomandazioni fornite saranno riportate in specifici report: Executive Summary, Technical Report e Remediation Plan (§5.2) • **Re-test delle vulnerabilità**: successivamente all'esecuzione delle azioni di rimedio delle vulnerabilità identificate, riportate all'interno del piano di rientro, potranno essere pianificate e svolte attività di re-test per verificare in maniera efficace la risoluzione delle vulnerabilità sui target analizzati e la mitigazione dei rischi connessi.

**5.1.1 STRUMENTI E SOLUZIONI TECNOLOGICHE.** Di seguito sono riportati i principali strumenti/soluzioni tecnologiche che saranno utilizzati per l'erogazione del servizio. Gli strumenti/tool di analisi riportati di seguito sono da intendersi a titolo non esaustivo. Nel corso delle attività, anche in considerazione dell'evoluzione delle minacce cyber, dell'utilizzo di tecnologie specifiche da parte dell'Amministrazione nonché dell'evoluzione del processo tecnologico potranno essere utilizzati ulteriori strumenti al fine di garantire un livello di qualità elevato nel corso delle attività.

Ambito di utilizzo	Principali strumenti
Vulnerability Assessment	• <b>Open Source</b> : Kali Linux, nmap, netdiscovery, dnsrecon, dig, metasploit, netcat, masscan, Shodan, Zoomeye, Censys, Air-Ng tools, Wifite, Airededdon, Wireshark. • <b>Di Mercato</b> : Nessus, Hak5 WiFi, Burp Proxy Professional. • <b>Proprietario</b> : Bug Blast
Cloud Security Assessment	• <b>Di Mercato</b> : Cloud Security Posture Management (CSPM), SaaS Security Posture Management (SSPM)
Vulnerability Assessment IoT	• <b>Open Source</b> : Blue Scanner, Blue Sniff, BlueBugger, BTBrowser, BTCrawler, BlueSnarfing, HackRF (HW), ZigDiggity, Proxmark (HW), TLSAssistant. • <b>Di Mercato</b> : Burp Proxy Professional

**5.2 PROPOSTA DI REMEDIATION PLAN E REPORTISTICA DI SINTESI E DETTAGLIO.** A seguito delle attività svolte in ambito Vulnerability Assessment sarà predisposta la reportistica necessaria a fornire all'Amministrazione una visione Executive, nonché tecnica, dello stato di sicurezza dei target oggetto di analisi. Di seguito sono forniti gli elementi distintivi della nostra reportistica:

Deliverable	Contenuti esemplificativi
VA Executive Summary	Report direzionale, con vista Executive, pensato per fornire una visione concreta al Management dello stato di sicurezza del/i target. Tale report conterrà un riepilogo generale delle attività eseguite e sintetizzerà i risultati ottenuti. Nello specifico: • Sintesi delle attività svolte e dei sistemi sottoposti ad analisi, con informazioni relative alla loro criticità per l'Amministrazione nonché di eventuali impatti normativi (es. GDPR); • Sintesi dei risultati con indicazione dei sistemi vulnerabili, aggregati per tipologia di vulnerabilità e livello di criticità (in termini qualitativi, ovvero il livello di vulnerabilità complessivo - alto, medio, basso – e quantitativo numero di vulnerabilità totali, critiche ed elevate). Saranno inoltre evidenziati gli impatti in ambito RID per l'Amministrazione in caso di ipotetico sfruttamento delle vulnerabilità da parte di un attaccante Cyber e le principali cause che portano alla presenza della vulnerabilità sul sistema/applicativo. Inoltre, sintesi dei risultati delle verifiche svolte sui servizi erogati dai Cloud Service Provider con indicazione precisa delle vulnerabilità rilevate, del livello di severità (qualitativo) e delle problematiche di sicurezza legate alla non adeguata configurazione dei servizi; • Sintesi delle azioni di rimedio – Classificate/prioritizzate in termini qualitativi (esecuzione nel breve, medio e lungo termine) definite a mitigazione delle vulnerabilità e rappresentazione del remediation plan con evidenza delle azioni prioritarie

VA Technical Report	Documento tecnico contenente un'analisi dettagliata e completa del livello di sicurezza, insieme a tutte le informazioni sulle vulnerabilità riscontrate (baseline), e relative azioni per mitigare o risolvere tali vulnerabilità. Il Technical Report è formato da resoconti analitici e grafici e contiene i seguenti elementi principali: <ul style="list-style-type: none"> <li>● Descrizione di dettaglio dei test di sicurezza eseguiti sui target in ambito (on premises - on cloud);</li> <li>● La lista di tutte le vulnerabilità riscontrate con indicazione di: nome della vulnerabilità sulla base del CVE (Common Vulnerabilities and Exposures), livello di severità in base alla probabilità di sfruttamento (alto, medio, basso) ed all'impatto legato allo sfruttamento della vulnerabilità (alto, medio, basso per Riservatezza, Integrità e Disponibilità - RID), dettagli tecnici sulla vulnerabilità rilevata ed evidenze documentali (con eventuale supporto di immagini e tabelle) delle attività svolte (comandi eseguiti e risposte dei sistemi). <b>Le informazioni dimensionali</b> per la valutazione delle vulnerabilità e delle relative remediation sono basate sul sistema di scoring delle vulnerabilità CVSS e sono principalmente le seguenti: <b>vettore di attacco, complessità di attacco, privilegi richiesti, tipologia di interazione dell'utente, possibilità di propagazione, impatti su confidenzialità, integrità e disponibilità</b>. Ciascuna delle dimensioni citate sono valorizzate su una scala dimensionale da 1 a 10, con una sintesi finale di rischio che può assumere i <b>seguenti valori qualitativi</b>: critico, alto, medio o basso.</li> </ul>
VA Remediation Plan	<b>Remediation plan</b> comprensivo delle iniziative tecniche da pianificare e svolgere per la mitigazione/risoluzione delle vulnerabilità identificate. Per ogni azione di rimedio sono fornite le seguenti <b>informazioni dimensionali</b> di dettaglio: attività da svolgere per la risoluzione delle vulnerabilità, complessità richiesta, nonché tempistiche dell'Amministrazione per l'esecuzione della stessa. Ciascuna delle dimensioni citate è valorizzata secondo le seguenti <b>informazioni qualitative</b> : tipologia di remediation (es: <i>R1-risoluzione completa</i> con azione da implementare, <i>R2-soluzione alternativa/compensativa/workaround</i> ), complessità per la risoluzione tecnica della vulnerabilità ( <i>C1-molto alto, C2-alto, C3-medio o C4-basso</i> ), tempistiche di risoluzione stimate ( <i>T1-ore, T2-giorni, T3-settimane o T4-mesi</i> con relativa proposta di pianificazione). Tali parametri sono determinati sulla base della collaborazione con i principali team operativi dell'Amministrazione impattati dalla vulnerabilità riscontrata e dall'azione di rimedio definita per la risoluzione. La determinazione di <b>Priorità nell'applicazione delle azioni di rimedio</b> è infine determinata dalla combinazione delle informazioni qualitative descritte e la <b>rischiosità della vulnerabilità</b> . Il parametro di Priorità risultante è espresso in termini di <i>P1-Critica, P2-Alta, P3-Media o P4-Bassa</i> .

**5.3 TEAM DI LAVORO.** Il team ottimale rispetterà i requisiti specificati nel CTS a cui si aggiungeranno i requisiti migliorativi sintetizzati di seguito.

Profilo	Requisito migliorativo generale
Security Principal, Senior Penetration Tester, Junior Penetration Tester	Nel team sarà inserita almeno una figura in possesso di una delle seguenti certificazioni aggiuntive: <b>eCPPT, GPEN, OSCP, eCPTX, OSCP, eCTHP, CRTP, OSWE, eWPT</b>

## 6 PROPOSTA PROGETTUALE PER I SERVIZI "TESTING DEL CODICE"

Il servizio di Testing del Codice prevede la rilevazione in maniera proattiva delle vulnerabilità presenti nel codice degli applicativi oggetto di analisi. Il RTI si impegna ad erogare le attività nel rispetto dei requisiti tecnico-funzionali specificati nel CTS, facendo affidamento sugli elementi distintivi sotto riportati:

**1. Adozione di una piattaforma SAST proprietaria**, specifica per l'acquisizione del codice e l'interazione con gli utenti finali, assicurando la generazione di **report standardizzati, confrontabili e soprattutto agnostici rispetto ai software di scansione adottati** (motori di scansione) **2. Metodologia per la definizione dei "remediation plan" con approccio risk-based** e reportistica in grado di rappresentare le vulnerabilità identificate sia ad interlocutori executive che tecnici, fornendo pratici strumenti operativi per agevolare la risoluzione delle stesse **3. Molteplici Centri di eccellenza sulla Sicurezza Applicativa e DevSecOps**, con la presenza di laboratori specialistici sulle attività di analisi statica (SAST) e dinamica (DAST) che analizzano costantemente le **nuove tecniche di sfruttamento delle vulnerabilità** con accesso ai più aggiornati dati di riferimento sulle stesse (es. Cyber Threat Intelligence e database con TTP utilizzate negli attacchi, segnalazione di API/librerie di terze parti vulnerabili) **4. Alleanze strategiche con i principali produttori mondiali di tecnologia per l'analisi statica/dinamica del codice** assicurando l'accesso privilegiato alle risorse tecniche degli stessi.

**6.1 MODALITA' DI ESECUZIONE DEL SERVIZIO.** La metodologia utilizzata per l'esecuzione delle attività richieste prevede la combinazione di strumenti automatici e verifiche manuali ed ha come obiettivo l'identificazione di vulnerabilità nel codice sorgente delle applicazioni analizzate. La modalità di esecuzione è concepita per garantire **risultati consistenti rispetto ad esecuzioni multiple successive sullo stesso applicativo**, fornendo dettagli specifici sulle vulnerabilità fino alla specifica sezione/linea di codice. Tale modalità rende il servizio efficace anche su analisi incrementali, adattandosi anche a contesti di sviluppo agile in cui si intende reiterare le analisi. Coerentemente, il servizio di testing del codice prevede sempre una fase iniziale di ispezione ed una seconda fase che ha l'obiettivo di verificare che le azioni di rimedio siano state implementate e risolutive. Le attività di Testing del Codice saranno eseguite mediante strumenti software open source, proprietari e/o di mercato, messi a disposizione dal RTI. Per soddisfare i requisiti indicati dall'Amministrazione procederemo, in coerenza con quanto definito dai principali standard di settore, all'esecuzione delle seguenti attività: **Analisi statica del codice (SAST), Analisi dinamica del codice (DAST), Mobile Testing**. Poiché, durante l'esecuzione delle attività (in particolare DAST e Mobile), il team potrebbe accedere a dati personali o sensibili dell'Amministrazione e dei cittadini, tali attività saranno costantemente monitorate per garantire l'impossibilità di esportare all'esterno tali dati. **Tutte le evidenze delle attività (es. log) saranno conservate dal RTI per un periodo garantito non inferiore a 1 mese dalla fine delle attività** e saranno rese disponibili, su richiesta, al personale autorizzato, **a garanzia di trasparenza operativa**. Tutte le informazioni, compresi i report tecnici, saranno inviate mediante **protocolli di cifratura e modalità condivise** durante la fase di "Analisi del contesto". L'esecuzione delle attività di Testing del codice richiede un coinvolgimento diretto dell'Amministrazione, che fornirà supporto per quanto concerne le fasi preliminari delle attività. Nello specifico l'Amministrazione supporterà la raccolta delle informazioni, nonché la documentazione tecnica necessaria per l'esecuzione dei test di sicurezza, tramite le seguenti attività:

- pianificazione e organizzazione di workshop operativi con gli stakeholder di riferimento (es. Applicativi, ICT) per la raccolta di informazioni utili all'esecuzione dei test
- raccolta della documentazione per l'esecuzione delle verifiche in white-box
- creazione di utenze di test con privilegi base per le verifiche di sicurezza (modalità gray-box)
- per le attività di analisi statica del codice, supporto per l'integrazione degli strumenti di analisi con i repository di progetto. Ove non possibile, invio, secondo

modalità sicure e concordate, del codice sorgente/binario che sarà oggetto di analisi. Per l'esecuzione delle attività da parte delle Amministrazioni, sulla base delle numerose progettualità eseguite in tale ambito, stimiamo un impegno medio di 2-3 gg/u ad esecuzione. Tale stima può variare sulla base della complessità dei target in scope nonché della complessità dell'Amministrazione stessa.

**Analisi statica del codice (SAST).** L'analisi statica del codice (SAST) mira ad identificare le vulnerabilità presenti nel codice sorgente. Tale attività è svolta in modalità white-box, richiedendo all'Amministrazione sia il codice sorgente dell'applicazione che la documentazione tecnica della stessa. Le attività sono eseguite principalmente sulla base dello standard OWASP Top 10 e tramite le seguenti tre fasi progettuali: **●FASE 1 - Analisi del contesto:** in tale fase si procede con la richiesta, raccolta e analisi della documentazione tecnica dell'applicazione (*analisi funzionale, workflow dell'applicazione, lista funzionalità, librerie terze parti utilizzate, architettura tecnica, ecc.*) e con l'acquisizione del codice sorgente **●FASE 2 – Secure Code Review:** esecuzione dell'analisi statica del codice sorgente dell'applicazione, ovvero: **▪ Configurazione dei tool di analisi** necessari per l'esecuzione delle attività sulla base delle caratteristiche del codice sorgente in ambito (es. linguaggio di programmazione) **▪ Code Scanning** mediante l'utilizzo di tool messi a disposizione dal RTI e selezionati sulla base delle caratteristiche dell'applicazione (es. linguaggio) ed in considerazione della complessità/criticità degli asset in oggetto. Gli strumenti che saranno messi a disposizione garantiranno la copertura di più di 20 linguaggi di programmazione e copriranno le vulnerabilità attualmente conosciute; **▪ Verifica manuale** delle evidenze fornite dai tool di scansione (manual code review) per la rilevazione ed eliminazione efficace dei falsi positivi ed identificazione di vulnerabilità di sicurezza per le funzionalità critiche; **▪ Assegnazione del livello di criticità** alle vulnerabilità rilevate in base alla probabilità di sfruttamento e del relativo impatto. L'assegnazione del livello di severità è fornita in primo luogo in maniera automatica dagli strumenti di analisi e rivisto dagli analisti di sicurezza. Il livello di severità è assegnato sulla base delle leading practice, delle policy di sicurezza dell'Amministrazione e di ulteriori fattori rilevanti (es. criticità dell'asset, rilevanza asset in ambito GDPR, facilità di sfruttamento della vulnerabilità, impatto della vulnerabilità, informazioni di CTI provenienti dai centri di eccellenza); **▪ Correlazione delle informazioni, identificazione azioni di rimedio, prioritizzazione e definizione del remediation plan.** **Le attività SAST di scansione periodica seguiranno un piano di verifica concordato con l'Amministrazione secondo modalità e tempistiche definite,** come ad esempio a seguito di major-change e/o mediante integrazione con i repository dell'Amministrazione (integrazione con pipeline CI/CD). L'esecuzione periodica delle attività consente il monitoraggio efficace dello stato di risoluzione delle vulnerabilità **● FASE 3 – Reporting:** predisposizione di report e dashboard con l'obiettivo di fornire una chiara visione sui risultati SAST e focalizzare l'attenzione sulla prioritizzazione delle vulnerabilità tecniche rilevate. Nello specifico sarà predisposto un Executive Summary e un Technical Report per singola esecuzione, evidenziando in maniera puntuale anche le aree di miglioramento.

**Analisi dinamica del codice (DAST).** L'analisi dinamica del codice (DAST) mira ad identificare le vulnerabilità delle applicazioni in runtime. Le attività sono eseguite sulla base dei principali standard OWASP Top 10 e OSSTMM, in modalità black-box e secondo tre macro-fasi tenendo conto del profilo dell'applicazione concordato (*Bronze, Silver, Gold*): **● FASE 1 - Analisi del contesto:** raccolta delle informazioni necessarie all'esecuzione dell'attività (e.g. nome applicazione, URLs) **● FASE 2 – Dynamic Security Testing:** esecuzione dell'analisi dinamica del codice sorgente dell'applicazione, ovvero: **▪ Configurazione dei tool di analisi** necessari per l'esecuzione delle attività sulla base delle caratteristiche dell'applicazione in scope **▪ Vulnerability Scan** dell'applicazione tramite strumenti open-source, proprietari e di mercato (ove necessario e su base periodica). Gli strumenti, opportunamente configurati sulla base delle leading practice e delle policy di sicurezza dell'Amministrazione, forniranno una valutazione automatica, in termini di severità/priorità, della vulnerabilità. Gli strumenti messi a disposizione garantiranno la copertura di più di 20 linguaggi e copriranno le vulnerabilità attualmente conosciute; **▪ Esecuzione di un'analisi di dettaglio** delle evidenze fornite dai tool di scansione per la rilevazione ed eliminazione dei falsi positivi ed esecuzione di un'analisi tecnica manuale per le funzionalità critiche; saranno eseguite verifiche di sicurezza specifiche sulla base del profilo assegnato all'applicazione in scope (*Bronze, Silver, Gold*). Nello specifico, a titolo non esaustivo, saranno eseguiti test di autenticazione (inclusi multilivello), autorizzazione, gestione della sessione, validazione degli input e manipolazione della logica applicativa, verifica dei messaggi di errore, protocolli utilizzati per le comunicazioni, meccanismi di logging e verifiche di compliance PCI-DSS; **▪ PoC Development** (profilo *Gold*): se richiesto e necessario, verranno dimostrate le limitazioni di sicurezza e le vulnerabilità identificate attraverso lo sviluppo di "Proof of Concept" in grado di far comprendere le modalità di realizzazione di uno scenario d'attacco da parte di un agente di minaccia specifico; **▪ Correlazione** delle informazioni, identificazione azioni di rimedio, prioritizzazione e definizione del remediation plan **● FASE 3 – Reporting:** predisposizione di report e dashboard con l'obiettivo di fornire una chiara visione sui risultati DAST e focalizzare l'attenzione sulla prioritizzazione delle vulnerabilità tecniche rilevate. Nello specifico sarà predisposto un Executive Summary e un Technical Report per singola esecuzione, evidenziando in maniera puntuale anche le aree di miglioramento.

**Mobile Testing.** Le attività di testing delle app mobile (Android, iOS, altri OS eventualmente richiesti) presuppongono l'esecuzione di attività sia di analisi statica che dinamica del codice. Rispetto alle attività identificate e descritte nei paragrafi precedenti, inoltre, le attività di testing delle app mobile presentano alcune peculiarità dovute alla natura delle app stesse (es. linguaggio utilizzato, librerie di terze parti, permessi richiesti al device), nonché ai device sui quali l'applicazione è installata (es. device con diritti di root/jailbreak). Per l'esecuzione dell'attività sarà richiesto di condividere il pacchetto eseguibile dell'applicazione (es. apk – Android, .ipa – iOS) e di creare credenziali di accesso per il testing. Le attività sono svolte sulla base dei principali standard, ad esempio *OWASP Mobile Security Testing Guide, OWASP Mobile Top 10, OWASP MASVS 1.1.3 (Level 2), OWASP API Security Top 10 e OSSTMM*. L'attività prevede le seguenti tre fasi progettuali: **●FASE 1 - Analisi del contesto:** analisi delle informazioni necessarie per l'esecuzione delle attività. Nello specifico richiesta, raccolta e analisi della documentazione tecnica dell'applicazione da analizzare (*analisi funzionale, workflow dell'applicazione, lista funzionalità, librerie terze parti utilizzate, architettura tecnica, ecc.*) e richiesta di creazione di un'utenza digitale per l'accesso all'app **● FASE 2 – Mobile Security Testing:** esecuzione del Security testing dell'app, ovvero: **▪ Configurazione dei tool di analisi** per l'esecuzione dell'attività (es. emulatori, tool di scanning); **▪ Application Mapping e manual vulnerability testing:** mappatura delle componenti dell'applicazione, verifica del corretto offuscamento del codice, analisi statica e dinamica del codice sorgente, delle API e delle interfacce verso altri sistemi mediante strumenti automatizzati. In tale fase sono inoltre svolti test di manipolazione della logica applicativa ed un'analisi delle policy di accesso ai dati ed alle funzioni del dispositivo da parte dell'applicazione. Esecuzione di un'analisi di dettaglio delle evidenze fornite dai tool di scansione per la rilevazione ed eliminazione dei falsi positivi ed esecuzione di un'analisi tecnica manuale per le funzionalità critiche. Le verifiche terranno conto inoltre delle informazioni provenienti dai centri di eccellenza del RTI relative a nuove vulnerabilità e librerie di terze parti vulnerabili; **▪ Assegnazione di un livello di criticità** alle vulnerabilità in base alla probabilità di sfruttamento e del relativo impatto. L'assegnazione del livello di severità sarà fornita in primo luogo in

maniera automatica dagli strumenti di analisi opportunamente configurati e successivamente rivisto dagli analisti di sicurezza. Il livello di severità è assegnato sulla base delle leading practice e delle policy di sicurezza dell'Amministrazione; ▪ **Correlazione** delle informazioni, identificazione azioni di rimedio, prioritizzazione e definizione del remediation plan • **FASE 3 – Reporting**: predisposizione di report e dashboard con l'obiettivo di fornire una chiara visione sui risultati del Mobile Testing e focalizzare l'attenzione sulla prioritizzazione delle vulnerabilità tecniche rilevate. Nello specifico sarà predisposto un Executive Summary e un Technical Report per singola esecuzione, evidenziando in maniera puntuale anche le aree di miglioramento.

**6.1.1 STRUMENTI E SOLUZIONI TECNOLOGICHE.** Di seguito sono riportati i principali strumenti/soluzioni tecnologiche che saranno utilizzati per l'erogazione del servizio. Gli strumenti/tool di analisi riportati di seguito sono da intendersi a titolo non esaustivo. Nel corso delle attività, anche in considerazione dell'evoluzione delle minacce cyber, dell'utilizzo di tecnologie specifiche da parte dell'Amministrazione nonché dell'evoluzione del processo tecnologico potranno essere utilizzati ulteriori strumenti al fine di garantire un livello di qualità elevato nel corso delle attività.

Ambito di utilizzo	Principali strumenti
Analisi statica del codice	• <b>Open Source</b> : SonarQube Community Edition, HCL Appscan Source Edition. • <b>Di Mercato</b> : Fortify, Checkmarx CxSAST. • <b>Proprietario</b> : GAST
Analisi dinamica del codice	• <b>Open Source</b> : HCLAppscan, Nikto, SQLMap, Ysoserial, CMSMap, WPScan, Dirbuster, Testssl.sh, SSLScan, Fiddler, Commix, FuzzDB. • <b>Di Mercato</b> : Microfocus WebInspect, Burp Suite Professional. • <b>Proprietario</b> : GAST
Mobile Testing (Android, iOS)	• <b>Android Application PT (Open source)</b> : Frida, Objection, MobSf, Apktool, Jadx, JD-GUI, Drozer, SWLite Browser, Android Studio e Platform Tools, Jar signer, Nox Emulator, Pidcat, Byte code viewer, Fri-dump, Dex2jar. • <b>iOS Application PT (Open Source)</b> : Class-dump, Frida, Objection, Radare2, Ghidra, FileDP, Filza, Passion Fruit, Needle, House, Clutch, Fri-dump, Xcode, Cycrit, dump_keychain, Otool. • <b>Dynamic Analysis</b> : Burp Suite Professional ( <b>Di Mercato</b> )

**6.2 PROPOSTA DI REMEDIATION PLAN E REPORTISTICA DI SINTESI E DETTAGLIO.** A seguito delle attività svolte in ambito Testing del codice sarà predisposta la reportistica necessaria a fornire all'Amministrazione una visione di alto livello e tecnica, dello stato di sicurezza delle applicazioni e delle vulnerabilità rilevate.

Report	Descrizione
Testing Codice Executive Summary	Report direzionale, con vista Executive, pensato per fornire una visione concreta al Management dello stato di sicurezza delle applicazioni. Tale report includerà un riepilogo generale delle attività eseguite e sintetizzerà i risultati ottenuti. Nello specifico: • Sintesi delle attività svolte e dei sistemi sottoposti ad analisi, con informazioni relative alla loro criticità per l'Amministrazione nonché di eventuali impatti normativi come GDPR; • Sintesi dei risultati con <b>indicazione dimensionali</b> relative a applicazioni vulnerabili, numero di debolezze/vulnerabilità totali, numero di debolezze/vulnerabilità differenziato per linguaggi, tipologie e stato (attivo, gestito, corretto, accettato, certificato, dismesso), aggregate per livelli di criticità (alto, medio, basso, informativo). • Sintesi delle azioni di rimedio definite a mitigazione delle vulnerabilità e rappresentazione del remediation plan con evidenza delle azioni prioritarie e delle tempistiche necessarie per l'implementazione delle stesse. L'Executive Summary potrà consentire al Management di acquisire informazioni utili per la revisione del PdS.
Testing Codice Technical Report	Documento tecnico contenente un'analisi dettagliata e completa del livello di sicurezza, insieme a tutte le informazioni sulle debolezze/vulnerabilità riscontrate, sulle modalità di sfruttamento e relative azioni per mitigare e, ove possibile, per eliminare tali debolezze/vulnerabilità. Il Technical Report è formato da resoconti analitici e grafici e contiene i seguenti elementi principali: • Descrizione di dettaglio dei test di sicurezza eseguiti sulle applicazioni in ambito; • La lista di tutte le debolezze/vulnerabilità riscontrate con indicazione di: nome della debolezza/vulnerabilità sulla base del CWE (Common Weakness Enumeration), descrizione estesa, conseguenza legata allo sfruttamento in termini di confidenzialità, integrità e disponibilità, riferimento alla linea di codice e raccomandazioni per la mitigazione o risoluzione. <b>Le informazioni dimensionali</b> per la valutazione delle vulnerabilità e delle relative remediation sono basate sul sistema di scoring delle vulnerabilità CVSS e sono principalmente le seguenti: <b>vettore di attacco, complessità di attacco, privilegi richiesti, tipologia di interazione dell'utente, possibilità di propagazione, impatti su confidenzialità, integrità e disponibilità</b> . Ciascuna delle dimensioni citate sono valorizzate su una scala dimensionale da 1 a 10, con una sintesi finale di rischiosità che può assumere i <b>seguenti valori qualitativi</b> : critico, alto, medio o basso.
Testing Codice Remediation Plan	<b>Remediation plan</b> comprensivo delle azioni di rimedio da pianificare e svolgere per la mitigazione/risoluzione delle debolezze (Weakness), vulnerabilità, configurazioni (con particolare riferimento al mobile testing) identificate. Per ogni azione di rimedio sono fornite le seguenti <b>informazioni dimensionali</b> di dettaglio: attività da svolgere per la risoluzione delle debolezze/vulnerabilità e complessità richiesta. Ciascuna delle dimensioni citate è valorizzata secondo le seguenti <b>informazioni qualitative</b> : tipologia di remediation (es: <i>R1-risoluzione completa con azione da implementare, R2-soluzione alternativa/compensativa/workaround</i> ), complessità per la risoluzione tecnica della debolezza/vulnerabilità ( <i>C1-molto alto, C2-alto, C3-medio o C4-basso</i> ). La determinazione di <b>Priorità nell'applicazione delle azioni di rimedio</b> è infine determinata dalla combinazione delle informazioni qualitative descritte e la <b>rischiosità della debolezza/vulnerabilità</b> . Il parametro di Priorità risultante è espresso in termini di <i>P1-Critica, P2-Alta, P3-Media o P4-Bassa</i> .
PoC vulnerabilità	Sviluppo di PoC delle vulnerabilità identificate per le applicazioni di profilo Gold a seguito delle attività di analisi dinamica del codice. Le PoC mostreranno uno scenario d'attacco da parte di un agente di minaccia specifico

**6.3 MODALITA' DI INTEGRAZIONE COL REPOSITORY SOFTWARE.** Il RTI propone l'adozione di una **piattaforma proprietaria specifica per l'acquisizione del codice** e l'interazione con il cliente. La Piattaforma GAST - **Global Application Security Testing** (§6.1.1) ha l'obiettivo di centralizzare le attività di SAST, fornire **report personalizzabili** e in formati **indipendenti dal software di scansione** utilizzato, governare scansioni incrementali e migliorare le modalità di rappresentazione e di interazione con l'Amministrazione. La piattaforma GAST consente un'**integrazione ottimale** con il ciclo di vita del codice, comprendendo i relativi repository *SVN - Subversion, CVS - Concurrent Versions System, Git, TFVC - Team Foundation Version Control*, mantenendo un **approccio "agnostico" rispetto ai vendor** utilizzati per la scansione. Tale modalità consente di utilizzare il **miglior software di scansione** a seconda di fattori quali caratteristiche delle



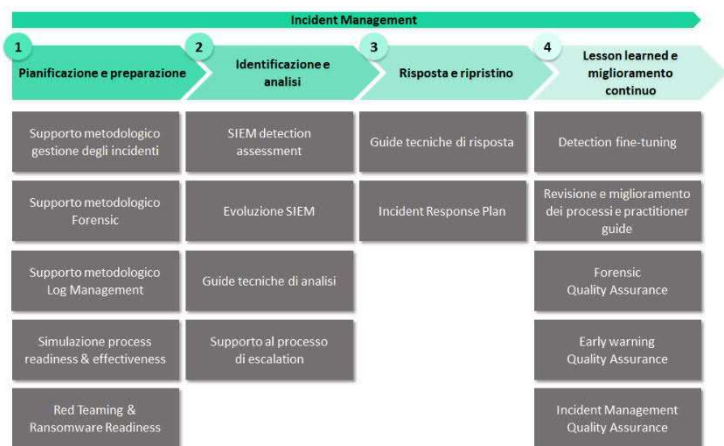
applicazioni, complessità e linguaggi di sviluppo, il tutto in **modalità trasparente per l'utente finale**. Tale modalità di erogazione è consigliata dal RTI, che tuttavia è disponibile ad adattare la stessa sulla base di eventuali esigenze delle Amministrazioni, concordandole di volta in volta con le stesse.

## 7 PROPOSTA PROGETTUALE PER IL SERVIZIO "SUPPORTO ALL'ANALISI E GESTIONE DEGLI INCIDENTI"

Il servizio di supporto all'analisi e gestione degli incidenti prevede lo svolgimento da parte del RTI di attività consulenziali volte a incrementare efficacia ed efficienza dei processi di Forensic e Incident Management, nelle fasi di analisi, progettazione e verifica (post-mortem) di tali processi, nonché di supporto alla divulgazione delle informazioni. Il RTI si impegna ad erogare le attività in ambito nel rispetto dei requisiti tecnico-funzionali specificati nel CTS, facendo affidamento sugli elementi distintivi elencati di seguito:

**1.** Coinvolgimento di **risorse con ampia e riconosciuta esperienza nella realizzazione di CERT e SOC** – strutture per le quali analisi e gestione degli incidenti sono servizi essenziali – in Italia e nel mondo per organizzazioni pubbliche e private di primaria importanza. **Il RTI ha inoltre supportato 7 delle 11 organizzazioni italiane che hanno accreditato i loro CERT alla community internazionale FIRST** **2.** Coinvolgimento di risorse che hanno contribuito direttamente allo **sviluppo delle pratiche di Incident Readiness** come dimostrato dalle pubblicazione di numerosi studi nazionali e internazionali, quali New Generation CERT: from Response to Readiness - Strategy and Guidelines (NATO, [https://www.nato.int/cps/en/natohq/news\\_140461.htm](https://www.nato.int/cps/en/natohq/news_140461.htm)), Linee guida per lo sviluppo e la definizione del modello nazionale di riferimento per i CERT regionali (AgID, <https://docs.italia.it/AgID/documenti-in-consultazione/lg-cert-regionali/it/bozza/index.html>) **3.** Disponibilità di una **libreria proprietaria composta da oltre 350 Use Case di monitoraggio costantemente aggiornata** sulla base delle esperienze acquisite presso i clienti del network a livello globale, evoluzioni tecnologiche, trasformazioni nelle tattiche, tecniche e procedure (TTP) utilizzate dagli attori di minaccia in diverse tipologie di ambienti (es. cloud SaaS, PaaS e IaaS, Mobile, IoT, ecc.) **4.** Disponibilità di **framework proprietari, sviluppati internamente dal RTI e aggiornati in maniera continuativa** sulla base delle esperienze acquisite e di report specialistici di settore, per la valutazione del livello di maturità di CERT e SOC e l'identificazione delle tecnologie di sicurezza a supporto delle attività di gestione degli incidenti **5. Team di lavoro multidisciplinare** altamente qualificato e certificato in ambito Forensic, Security Defense e Offense.

### 7.1 MODALITÀ DI ESECUZIONE DEL SERVIZIO, MODELLO ORGANIZZATIVO ADOTTATO E STRUMENTI. 7.1.1 MODALITÀ DI ESECUZIONE DEL SERVIZIO



servizio di supporto all'analisi e gestione degli incidenti proposto affronta la tematica in modo olistico e multidisciplinare, in modo da promuovere il miglioramento continuo della *Incident Readiness* dell'Amministrazione attraverso elementi quali la corretta definizione dei processi, un'adeguata formazione del personale e l'ingegnerizzazione delle tecnologie di sicurezza, fondamentali per garantire nel tempo efficacia, efficienza e tempestività al servizio remoto di Incident Management erogato dal fornitore del Lotto 1 (laddove attivato) o da altre terze parti coinvolte e far fronte alla costante evoluzione degli attacchi informatici e all'incremento delle tipologie degli ambienti in perimetro (es. servizi cloud, dispositivi mobile, IoT, ecc.). Al fine di raggiungere tali obiettivi, il RTI si candida a supportare l'Amministrazione al fine di (A) abilitare il corretto svolgimento di ciascuna delle fasi di gestione

degli incidenti attraverso attività consulenziali da svolgersi in maniera preventiva come supporto all'intero processo (analisi e progettazione) e (B) definire un processo strutturato di Forensic e verificarne l'efficacia (verifica). Tali attività saranno svolte in linea con i principali standard (es. ISO/IEC 27035, ISO/IEC 27002, NIST 800.61sp2), normative e linee guida di settore (es. DL 65/2018, DL 81/2021, Framework Nazionale per la Cybersecurity e la Data Protection), integrandosi inoltre con gli altri servizi del presente Lotto 2 e del Lotto 1, secondo quanto riportato all'interno del "Modello Correlazione Servizi", descritto all'interno del capitolo *Proposta progettuale per il servizio "Security Strategy"*.

**A. Incident Management.** Il RTI propone un approccio strutturato al supporto in ambito gestione incidenti, che prevede l'esecuzione di attività di natura consulenziale da svolgersi preventivamente per guidare il corretto svolgimento del servizio di Incident Management da parte dell'Amministrazione (direttamente, tramite servizi del Lotto 1 o altri fornitori). Ciascuna delle attività proposte consentirà di abilitare lo svolgimento e incrementare l'efficacia di una diversa fase del processo di Incident Management, come di seguito riportato: **A.1 Pianificazione e preparazione:** una fase di preparazione correttamente eseguita e personalizzata sulla base del contesto permette di minimizzare gli impatti degli incidenti, facendo leva su un'adeguata infrastruttura tecnologica di sicurezza e personale specializzato. **[Attività proposte]** • *Supporto metodologico gestione degli incidenti:* sviluppo e/o revisione di modelli operativi e processi strutturati di Incident Management, rispettivamente volti a guidare gli analisti di sicurezza nelle relative attività quotidiane, e definire ruoli, responsabilità, principi e attività operative che regolano il processo stesso, in linea con quanto prescritto dal CSIRT-Italia. Tale formalizzazione del processo prevede anche la definizione di obiettivi, modello organizzativo, criteri di classificazione di un incidente – sulla base della criticità intrinseca della minaccia e della rilevanza dell'asset – criteri di escalation (lista di contatti degli attori da coinvolgere e relativa modalità di notifica in base alla criticità dell'evento), input, output e interrelazioni delle varie attività, metriche di riferimento (KPI) per la misurazione dell'efficacia, oltre all'integrazione con processi esterni (es. gestione di data breach, gestione delle crisi, ecc.) e alle modalità di comunicazione/aggiornamento verso entità interne ed esterne (ivi incluse escalation verso Amministrazione centrale/periferica, altre amministrazioni, CSIRT-Italia, Organi di Polizia, richiesta di approfondimenti presso il fornitore del servizio di Threat intelligence e Vulnerability data feed, laddove attivato, ecc.); • *Supporto metodologico Forensic:* sviluppo e/o revisione di processi strutturati di analisi forense volti a guidare gli specialisti nelle relative attività, come dettagliato all'interno del paragrafo successivo "B. Forensic"; • *Supporto metodologico Log Management:* sviluppo e/o revisione di una policy strutturata di Log Management al fine di standardizzare la raccolta e centralizzazione dei log da parte dell'amministrazione, definendo un livello standard di *logging* per ciascuna fonte, al fine di supportare le attività di analisi degli eventi; • *Simulazione Process readiness & effectiveness:* svolgimento di simulazioni interattive (es. table-top) di attacchi cyber realistici basati sugli scenari di minaccia più frequenti al fine di verificare la conoscenza del

processo in ambito e la capacità degli attori coinvolti di gestire tali eventi. A supporto di queste attività il RTI mette a disposizione dell'Amministrazione spazi innovativi che renderanno possibile, mediante l'utilizzo di tecnologia di avanguardia, la realizzazione di laboratori esperienziali di simulazione "reale" (es. EY Wavespace); • **Red Teaming & Ransomware Readiness**: svolgimento, in sinergia con il servizio di "Penetration Testing" (vedi capitolo *Proposta progettuale per il servizio "Penetration Testing"*), di attività di Red Teaming e Ransomware Readiness al fine di testare, rispettivamente, l'efficacia dei processi di rilevazione e risposta alle minacce cyber e il livello di resilienza dell'Amministrazione nei confronti delle minacce di tipo ransomware identificando eventuali gap di sicurezza, incrementando la postura di sicurezza complessiva e le capacità di risposta a tali incidenti. **A.2 Identificazione e analisi**: la fase di identificazione e analisi di un incidente ha l'obiettivo di monitorare in modo centralizzato gli eventi di sicurezza provenienti da fonti strutturate (es. SIEM) e non strutturate (es. e-mail da utenti) per rilevare minacce miranti agli asset e ai servizi della PA, analizzarli per comprendere se si tratti di un falso positivo che necessita di azioni correttive o di un incidente con potenziale impatto sul perimetro e classificare e prioritizzarne la gestione sulla base di criteri definiti. **[Attività proposte]** • **SIEM detection assessment**: valutazione delle capacità di rilevazione delle minacce sulla base della visibilità offerta da regole e Use Case di monitoraggio implementati e relative sorgenti, sulla base di framework di settore (es. MITRE ATT&CK), in presenza di una piattaforma SIEM già esistente o nel caso di attivazione di un servizio SOC esterno; • **Evoluzione SIEM**: definizione di Use Case di monitoraggio volti a incrementare la capacità di rilevazione di potenziali incidenti, sulla base dei risultati dell'assessment di cui al punto precedente e di una vasta libreria di Use Case; • **Guide tecniche di analisi**: sviluppo e/o revisione di guide *step-by-step* (*practitioner guide*) che orientino le attività di analisi dei log e degli eventi a valle dell'identificazione di un potenziale incidente di sicurezza e di ricerca proattiva delle minacce (*Threat Hunting*), al fine di incrementare l'efficienza del processo di monitoraggio e la visibilità sugli scenari di minaccia di interesse; • **Supporto al processo di escalation**: supporto all'Amministrazione nel coordinamento della comunicazione e dell'invio di notifiche/aggiornamenti circa incidenti verso le autorità competenti (es. Organi di Polizia) laddove necessario, ivi incluse la segnalazione di potenziali data breach, in ottemperanza a quanto previsto dalla normativa GDPR, e la notifica degli incidenti aventi un impatto rilevante sui servizi essenziali e digitali verso il CSIRT-Italia, nelle modalità previste dal D.lgs 65/2018 (attuazione Direttiva NIS) e dal decreto n. 81/2021. **A.3 Risposta e ripristino**: tale fase prevede l'identificazione e l'implementazione delle azioni di contenimento a breve termine dell'incidente, eradicazione della minaccia e ripristino dei sistemi impattati, con l'obiettivo di limitare le conseguenze dell'incidente e ripristinare la normale operatività in maniera tempestiva ed efficace. **[Attività proposte]** • **Supporto specialistico nell'elaborazione e nel coordinamento dell'implementazione di una strategia di risposta e ripristino per la corretta gestione degli incidenti**. L'approccio prevede: • **Guide tecniche di risposta**: definizione di guide *step-by-step* (*practitioner guide*) per la gestione degli incidenti noti a bassa criticità, che consentano di uniformare e semplificare la gestione di casistiche simili da parte del team di Incident Management (interno o esterno all'Amministrazione), abilitando l'eventuale implementazione di automatismi utili a focalizzare le proprie risorse sulle attività a valore aggiunto e di incrementare l'efficienza dei task più ripetitivi; • **Incident Response Plan**: definizione di linee guida e strumenti operativi (template) per la gestione di incidenti complessi ad alta criticità da parte del team di Incident Management (interno o esterno all'Amministrazione), al fine di mitigare gli impatti causati dagli stessi. Tale template consentirà di prioritizzare le attività di risposta e ripristino in base alla natura dell'incidente (concluso oppure in corso con persistenza dell'attaccante), utilizzando come input le valutazioni sulla riduzione del rischio e l'effort di implementazione richiesto. **A.4 Lesson learned e miglioramento continuo**: tale fase prevede, immediatamente a valle della gestione di un incidente, una valutazione ex-post della stessa per verificare che le attività siano state condotte in conformità con quanto previsto dal processo, e un'attività periodica volta a identificare eventuali punti di miglioramento nelle attività svolte attraverso l'elaborazione di reportistica, lo svolgimento di meeting ricorrenti per condividere eventuali gap e relative azioni di rimedio. **[Attività proposte]** • **Detection fine tuning**: supporto al processo di fine tuning della capacità di rilevazione delle minacce al fine di ridurre il numero di falsi positivi individuati, definendo anche le eventuali azioni di remediation utili a ridurre la probabilità di occorrenza attraverso modifiche: • agli Use Case di monitoraggio in termini di logica e soglie di allarme • alle ulteriori tecnologie interessate, qualora le cause siano indipendenti dalla piattaforma di monitoraggio (es. correzione delle configurazioni errate delle sorgenti); • **Revisione e miglioramento dei processi e practitioner guide**: sulla base delle risultanze delle lesson learned e delle ulteriori attività del Lotto 2 (es. Vulnerability Assessment, Penetration Testing, ecc.), oltre che delle informazioni contenute all'interno dei bollettini ricevuti dal CSIRT-Italia; • **Forensic quality assurance**: svolgimento di attività di *quality assurance* del processo di Forensic, come dettagliato all'interno del paragrafo successivo "B. Forensic"; • **Early Warning quality assurance**: definizione di una checklist che consenta di svolgere attività di *quality assurance* sul processo di ricezione e verifica di bollettini e informazioni in merito a rischi e incidenti emessi dal CSIRT-Italia; • **Incident Management quality assurance**: governo (organizzazione, pianificazione, coordinamento, controllo) delle attività di verifica tecnica dei servizi di Incident Management erogati tramite il Lotto 1 o da altri fornitori. Il RTI, grazie alle proprie competenze in tema di *assurance* di servizi di sicurezza, potrà supportare le attività di verifica dei risultati attesi. **B. Forensic**. Le attività di supporto all'Amministrazione nella gestione di incidenti di sicurezza prevedono un approccio sinergico, finalizzato a incrementare l'efficienza delle modalità di intervento e dei tempi di reazione da parte dell'Amministrazione, in particolare nell'analisi forense post-mortem degli incidenti. Le attività di supporto erogate nei confronti dell'Amministrazione prevedranno una costante verifica di *quality assurance* da parte di profili esperti, al fine di garantire un elevato livello qualitativo dell'esecuzione del processo di Forensic. **[Attività proposte]** • **Definizione di un template catena di custodia per supportare i team di Forensic nel tracciamento delle attività eseguite sulle evidenze acquisite**; • **Definizione di un processo di Forensic secondo best practice** volto a definire ruoli, responsabilità, principi e attività operative che regolano il processo stesso; • **Governo** (organizzazione, pianificazione, coordinamento, controllo) delle attività di verifica tecnica (*quality assurance*) del processo di Forensic. Il processo di Forensic, in via generale, può astrattamente essere declinato nei seguenti step, per ciascuno dei quali sono riportate le attività principali il cui corretto svolgimento verrà verificato e valutato dal RTI, sulla base del processo definito: • **Assessment iniziale**, rilevazione preliminare del contesto specifico, necessaria a identificare la strategia di intervento più idonea ed efficiente in base alla tipologia di incidente rilevato. Durante tale step, sono di norma raccolte tutte le informazioni immediatamente disponibili e necessarie ad ottenere una ricostruzione sommaria del caso (es. inquadramento cronologico della vicenda). Nel corso di tale step sono altresì individuate le risorse con competenze specifiche da includere nella composizione di un team dedicato interdisciplinare, che può includere, a titolo esemplificativo, profili tecnici, legali e esperti di data protection. Infine, deve essere identificato il perimetro dei sistemi potenzialmente rilevanti su cui condurre i successivi approfondimenti tecnici (es. endpoint utente, server e apparati di rete, server, log applicativi, copie di caselle e-mail, ecc.), target dello step di *data collection*; • **Data collection** acquisizioni di evidenze informatiche ("ESI"), svolte preservando l'integrità delle fonti dati originali e garantendo allo stesso tempo la validità

probatoria dei dati acquisiti (copie forensi) attraverso l'uso di procedure e strumenti certificati secondo le best practice internazionali di Forensic. Le acquisizioni in parola devono essere accompagnate dalla produzione di idonea documentazione, necessaria a documentare i processi operati durante le acquisizioni stesse, oltre che a tracciare la catena di custodia (*chain of custody*) delle evidenze acquisite. Tale attività viene condotta mediante una precisa descrizione del processo di trasferimento delle evidenze, dettagliando il materiale raccolto, gli attori coinvolti, i riferimenti temporali e i luoghi dei trasferimenti. ■ **Investigazione,** svolgimento di analisi tecniche sulle evidenze informatiche acquisite, diversificate in base alla peculiarità del caso di specie. In considerazione della varietà delle tipologie di incidenti di sicurezza, oltre che della specificità dei sistemi coinvolti, possono essere eseguite attività di (i) analisi dei log e degli eventi, finalizzate alla comprensione della natura dell'incidente e delle Tattiche, Tecniche e Procedure (TTP) adottate dal potenziale agente di minaccia e alla rilevazione degli Indicatori di Compromissione (IoC) necessari per una ricostruzione della timeline dell'incidente, individuare eventuali esfiltrazioni di dati e comprendere le root-cause dell'accaduto; (ii) *Malware Analysis & Forensic*, volte a estrarre Indicatori di Compromissione (IoC) unici e non precedentemente noti da malware e altri software malevoli attraverso attività di *reverse engineering* del codice e analisi statiche e dinamiche; (iii) *threat hunting* e *threat actor cyber intelligence*, aventi l'obiettivo di anticipare proattivamente le operazioni malevole di eventuali agenti di minaccia e reperire informazioni su di essi.

**7.1.1.1 DELIVERABLE.** Considerata la natura delle attività consulenziali previste, sono riportati di seguito esclusivamente a **titolo esemplificativo e non esaustivo** alcuni dei deliverable previsti come risultanza del servizio.

Deliverable	Contenuti esemplificativi
Processo di Incident Management	Documento che ha l'obiettivo di descrivere tutte le attività del processo. Esso si compone, al minimo, delle seguenti sezioni: obiettivo e ambito di applicazione, workflow di processo, descrizione attività e attivazione processi esterni, matrice di escalation e modalità di comunicazione, matrice di classificazione, matrice RACI per identificazione di ruoli e responsabilità e metriche e KPI di processo.
Processo di analisi forense	Documento che ha l'obiettivo di descrivere tutte le attività del processo. Esso si compone, al minimo, delle seguenti sezioni: obiettivo e ambito di applicazione, workflow di processo, descrizione attività e attivazione processi esterni, modalità di comunicazione, matrice RACI per identificazione di ruoli e responsabilità e metriche e KPI di processo.
SIEM detection assessment	Presentazione di dettaglio delle analisi svolte per valutare le capacità di detection di una piattaforma SIEM, composta da un'analisi AS-IS degli Use Case implementati, rappresentata all'interno di una <i>heatmap</i> basata sul framework MITRE ATT&CK, e da una roadmap che consenta di incrementare la visibilità e le capacità di rilevazione delle minacce, attraverso nuovi Use Case da implementare ed eventuali nuove sorgenti da integrare con il SIEM.
<i>Practitioner guide</i> gestione incidenti e Incident Response Plan (IRP)	Sviluppo di procedure tecniche di dettaglio utili a guidare le attività del team operativo in caso di incidenti noti non critici ad alta frequenza, al fine di ridurre i tempi di risposta e di limitare gli errori nella loro gestione, individuando lo scenario dell'incidente, una strategia di risposta su tre livelli (strategico, tattico, operativo) e una descrizione delle azioni da svolgere per ciascun livello, con identificazione dei ruoli coinvolti, e di un template utile a guidare la definizione delle attività di risposta al verificarsi di un incidente ad alta criticità, comprendente informazioni sullo stato di avanzamento, la struttura <i>accountable</i> e l'attore <i>responsible</i> per ciascuna attività, e la priorità associata con relativa <i>due date</i> .

**7.1.2 MODELLO ORGANIZZATIVO ADOTTATO E STRUMENTI. 7.1.2.1 MODELLO ORGANIZZATIVO.** Il modello prevede un team di progetto guidato da un Project Manager (Security Principal) che avrà lo scopo di definire, in accordo con l'Amministrazione, le tempistiche e le milestone progettuali. Tale risorsa coordinerà lo svolgimento delle differenti attività, garantendo il raggiungimento degli obiettivi e assicurando in particolar modo che le competenze del Forensic Expert siano pienamente integrate nello svolgimento delle attività, a supporto delle ulteriori figure individuate. Senior e Junior Security Analyst, figure con un background tecnico, e con ampia esperienza in attività consulenziali in ambito Incident Management e Forensic, consentiranno di assicurare un alto livello di qualità dei deliverable relativi alle fasi di analisi, progettazione e verifica dei processi, avvalendosi del supporto specialistico del Forensic Expert in particolare durante le attività di quality assurance del processo di Forensic. **Ove necessario il RTI potrà accedere a competenze e risorse ulteriori disponibili all'interno del proprio network per attività che richiedano professionalità differenti da quelle incluse all'interno del team di lavoro.** **7.1.2.2 STRUMENTI IN AMBITO ANALISI FORENSE** Nel corso delle attività il RTI utilizzerà la propria Knowledge Base di processi e *practitioner guide*, sviluppati nell'ambito di numerose progettualità, utili a fornire una baseline di riferimento per i deliverable corrispondenti. Considerata la tipologia di attività in ambito al servizio, non risultano necessari strumenti e soluzioni tecnologiche per lo svolgimento delle stesse. Ciononostante, il RTI ha comprovata esperienza nell'utilizzo dei seguenti strumenti/soluzioni tecnologiche: ● **Data collection:** OpenText EnCase, AccessData FTK, Cellebrite UFED, Sumuri Paladin, Tableau Write Blocker, Duplicator; ● **Analisi dei Log e degli eventi:** DeepBlue, Yara, EvtxParser, Autopsy; ● **Malware Analysis & Forensic:** Ida Pro, x96dbg, PE Studio, Sandbox proprietarie del RTI; ● **Threat Actor Cyber Intelligence:** piattaforme proprietarie del RTI, TheHive, MISP, MineMeld; ● **Threat Hunting:** Wazuh, Wireshark, Kape, Redline, agenti EDR (es. CrowdStrike, Cybereason, etc.).

**7.2 PROPOSTA DEL DOCUMENTO DI CATENA DI CUSTODIA** Il documento *catena di custodia* permette all'Amministrazione di tracciare cronologicamente tutte le attività eseguite sui diversi elementi di prova raccolti e gli attori che hanno portato a termine tali attività. All'interno di questo template, in linea con lo standard ISO/IEC 27037, è inclusa una descrizione di dettaglio dei dispositivi oggetto di custodia e una serie di informazioni relative alle operazioni eseguite su di essi da uno o più attori (es. riferimenti temporali, identificativo dell'attore, operazioni tecniche eseguite), in un formato standardizzato al fine di facilitarne la compilazione. Il documento *catena di custodia* è costituito da una sezione iniziale dedicata alla descrizione puntuale e dettagliata dei device/evidenze oggetto di custodia (es. quantità, marca, modello, s/n, eventuali altri ID, tag, custodian assegnatario) e da una sezione dedicata ai vari passaggi di custodia dei device/evidenze di cui al punto precedente nella quale saranno documentate l'insieme delle **informazioni dimensionali** e **qualitative** di seguito riportate: [i] tutti i riferimenti dei soggetti coinvolti (es. nome, cognome, società e ruolo), [ii] la firma autografa da parte degli stessi, [iii] i riferimenti temporali (data e ora) e dei luoghi (indirizzo e descrizione) dei passaggi, [iv] le motivazioni sottostanti le movimentazioni (es. presa in carico per acquisizione), [v] la presenza di eventuali sigilli, oltre che [vi] eventuali ulteriori note ed infine [vii] una sezione dedicata alla sigla di una terza parte per Quality Control. Al momento della cristallizzazione di una evidenza digitale viene inoltre creato un modulo denominato Evidence acquisition dove sono memorizzate tutte le informazioni relative al processo di

cristallizzazione, quali: i beni cristallizzati, gli strumenti utilizzati (marca, modello, versione, configurazione), i dati di processo (data e ora inizio e fine attività, luogo, operatore, hash delle evidenze, eventuali anomalie) e i supporti su cui vengono immagazzinate le informazioni (target e backup).

**7.3 TEAM DI LAVORO.** Il team ottimale rispetterà i requisiti specificati nel CTS a cui si aggiungeranno i requisiti migliorativi sintetizzati di seguito.

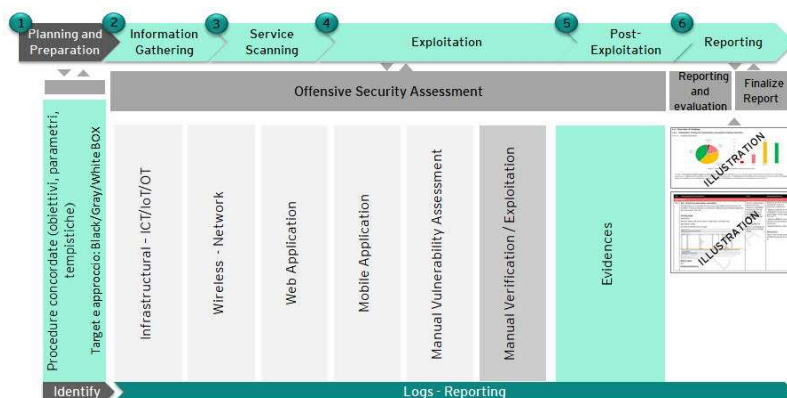
Profilo	Requisito migliorativo generale
Security Principal, Senior Security Analyst, Junior Security Analyst, Forensic Expert	Nel team sarà inclusa almeno una risorsa con certificazione <b>CISSP o CISM o Lead Auditor ISO 27001</b> .

## 8 PROPOSTA PROGETTUALE PER IL SERVIZIO “PENETRATION TESTING”

Il servizio di Penetration Test prevede l'esecuzione di attacchi simulati per verificare concretamente la possibilità di sfruttare vulnerabilità identificate su sistemi/reti/applicazioni/dispositivi delle Amministrazioni. L'approccio offensivo consente di ottenere una chiara percezione degli effettivi livelli di esposizione/compromissione dei target analizzati, determinando la capacità di difesa e resilienza rispetto agli attacchi Cyber e fornendo conseguentemente elementi concreti per adeguare le misure di contrasto e protezione. Il servizio proposto è fondato sugli elementi distintivi sotto riportati:

**1. Eccellenza del team di Ethical Hacking** dimostrata dalla **pubblicazione regolare di Common Vulnerabilities and Exposures (CVE)** elenco di vulnerabilità divulgate pubblicamente e *Zero Day*, condivise attraverso i metodi di "Responsible Disclosure" (oltre 17 negli ultimi due anni, ad esempio *CVE-2020-15307*, *CVE-2020-7049*, *CVE-2020-0962*, *CVE-2020-0784*); **2. Copertura completa dei principali vettori di attacco per ogni singola sessione** e tipologia di target, acquisita mediante l'aggiornamento continuo di un **archivio centralizzato contenente il Threat Modelling e relative Tactics, Techniques and Procedures (TTP)**, alimentato dal team di Pen Tester coinvolti a livello globale nell'erogazione di tali servizi (**oltre 17.000 test effettuati annualmente da oltre 1.300 Pen tester**); **3. Utilizzo estensivo di fonti Cyber Threat Intelligence (OSINT e CLOSINT)** con copertura geografica mondiale, derivante dai servizi di sicurezza gestista (SOC) del RTI, che consentono al Pen Tester di ottenere un quadro più ampio dell'effettivo livello di esposizione dei target in analisi, come ad esempio compromissioni/vulnerabilità/tecniche pubblicate nel dark web o in community specifiche, potenzialmente accessibili anche agli attaccanti e sfruttabili per realizzare una reale compromissione. Inoltre, tale capacità consente di **stabilire se i target oggetto di analisi siano stati precedentemente compromessi o attenzionati** da organizzazioni e/o singoli attaccanti; **4. Molteplicità di laboratori a livello nazionale ed internazionale (oltre 10 in Europa)** con personale, strumenti ed infrastrutture dedicate alle attività di offensive security, con possibilità di **verificare costantemente i vettori e le tecniche di attacco in ambienti simulati e su dispositivi di test** (IoT, Mobile, sistemi Embedded, riproduzione di sistemi ICS/OT); tali laboratori sono impiegati anche per **addestramento, formazione ed aggiornamento continuo dei Pen Tester**.

**8.1 MODALITA' DI ESECUZIONE DEL SERVIZIO E CAUTELE ADOTTATE.** Le attività di PT sono basate principalmente sulle metodologie OSSTMM, OWASP e PTES, riconosciute globalmente come standard de-facto, che guideranno la conduzione dell'analisi in termini di fasi da rispettare e test da effettuare. L'applicazione di tali metodologie garantirà test condotti accuratamente sui Target e **risultati consistenti, ripetibili e misurabili**. Il servizio può assumere tre diverse declinazioni in relazione alla combinazione di diversi fattori come la tipologia dei target, risultati delle analisi pregresse condotte sugli stessi, i vettori di attacco e le modalità di esecuzione (white, gray, black box) impiegabili: • **PT su Infrastrutture:** si analizzano ad esempio componenti di rete come router, switch, servizi di rete (Domain Controller, SSH Server, FTP Server, Web Server, ...), infrastrutture wireless (Wi-Fi); • **PT su Applicazioni:** analisi svolte su applicazioni ad esempio Web, API, Mobile e Thin Client; • **PT su Dispositivi:** analisi svolte ad esempio su dispositivi IoT, sistemi "embedded", dispositivi industriali. Le attività di PT saranno eseguite in modalità **Black-box** (verifica del livello di sicurezza dei target senza alcuna credenziale di accesso – test non autenticato), **Gray-box** (verifica del livello di sicurezza dei target simulando un attaccante che possiede una parziale conoscenza dell'infrastruttura oggetto di analisi e credenziali di accesso con privilegi base – test autenticato) e **White-box** (verifica del livello di sicurezza dei target con conoscenze dettagliate sull'infrastruttura/applicazione oggetto di analisi e credenziali con privilegi avanzati). La metodologia adottata per l'esecuzione dei PT prevede 6 fasi: *Planning and Preparation*, *Information Gathering*, *Service Scanning*, *Exploitation*, *Post-exploitation*, *Reporting*. Le attività di PT potranno essere eseguite come singole campagne o in modalità ricorrente sulla base delle necessità espresse e concordate con le Amministrazioni. Il RTI è in grado di erogare anche servizi di **Red Teaming** che affiancano ai test sulle componenti IT - utilizzando tecniche analoghe al PT -, test della componente fisica e personale, mediante tecniche di Social Engineering. Questa tipologia di servizio impiega un approccio a scenari utilizzando una serie di tecniche che mirano a rendere invisibili e "silenziosi" gli attacchi. Ciò permette di verificare l'efficacia delle soluzioni di protezione posta a difesa del target oggetto del servizio e allo stesso tempo dei livelli di difesa messi in atto dal team di sicurezza dell'Amministrazione (Blue Team). In alcuni scenari è contemplata la possibilità di coordinamento tra team di difesa (Blue Team) e di attacco (Red Team) per costituire un Purple Team che, da un lato supporta il Red Team nei suoi attacchi, e dall'altro suggerisce strategie difensive al Blue Team. Le attività di Red Teaming rappresenta un'attività addizionale e migliorativa rispetto a quanto previsto dal CTS di gara. A supporto inoltre del miglioramento della sicurezza del patrimonio informativo aziendale, potranno essere svolte simulazioni di **Phishing**, eseguite singolarmente o in combinazioni con altre attività/servizi. Le attività consistono nella simulazione di invio mail fraudolente con lo scopo di verificare la preparazione degli utenti e aumentarne la consapevolezza rispetto alle minacce Phishing. Può essere altresì utilizzato in maniera avanzata per simulare attacchi client-side più complessi che prevedono di veicolare un malware all'interno dell'azienda. **CAUTELE ADOTTATE NELL'ESECUZIONE DEL SERVIZIO:** Il team di verifica - durante l'esecuzione delle attività - potrebbe ottenere l'accesso a dati personali o sensibili delle Amministrazioni e dei cittadini. In ragione di questo le attività **saranno costantemente monitorate** per garantire l'impossibilità di esportare all'esterno tali dati. Inoltre, **le attività di test saranno tracciate attraverso**



La metodologia adottata per l'esecuzione dei PT prevede 6 fasi: *Planning and Preparation*, *Information Gathering*, *Service Scanning*, *Exploitation*, *Post-exploitation*, *Reporting*. Le attività di PT potranno essere eseguite come singole campagne o in modalità ricorrente sulla base delle necessità espresse e concordate con le Amministrazioni. Il RTI è in grado di erogare anche servizi di **Red Teaming** che affiancano ai test sulle componenti IT - utilizzando tecniche analoghe al PT -, test della componente fisica e personale, mediante tecniche di Social Engineering. Questa tipologia di servizio impiega un approccio a scenari utilizzando una serie di tecniche che mirano a rendere invisibili e "silenziosi" gli attacchi. Ciò permette di verificare l'efficacia delle soluzioni di protezione posta a difesa del target oggetto del servizio e allo stesso tempo dei livelli di difesa messi in atto dal team di sicurezza dell'Amministrazione (Blue Team). In alcuni scenari è contemplata la possibilità di coordinamento tra team di difesa (Blue Team) e di attacco (Red Team) per costituire un Purple Team che, da un lato supporta il Red Team nei suoi attacchi, e dall'altro suggerisce strategie difensive al Blue Team. Le attività di Red Teaming rappresenta un'attività addizionale e migliorativa rispetto a quanto previsto dal CTS di gara. A supporto inoltre del miglioramento della sicurezza del patrimonio informativo aziendale, potranno essere svolte simulazioni di **Phishing**, eseguite singolarmente o in combinazioni con altre attività/servizi. Le attività consistono nella simulazione di invio mail fraudolente con lo scopo di verificare la preparazione degli utenti e aumentarne la consapevolezza rispetto alle minacce Phishing. Può essere altresì utilizzato in maniera avanzata per simulare attacchi client-side più complessi che prevedono di veicolare un malware all'interno dell'azienda. **CAUTELE ADOTTATE NELL'ESECUZIONE DEL SERVIZIO:** Il team di verifica - durante l'esecuzione delle attività - potrebbe ottenere l'accesso a dati personali o sensibili delle Amministrazioni e dei cittadini. In ragione di questo le attività **saranno costantemente monitorate** per garantire l'impossibilità di esportare all'esterno tali dati. Inoltre, **le attività di test saranno tracciate attraverso**



**un sistema di registrazione delle sessioni dei tester (i.e. Key logging o recording sessioni RDP) a garanzia di trasparenza operativa.** Tale tracciamento potrà essere reso disponibile all'Amministrazione su richiesta o conservato dal RTI sulla base del periodo di Retention che sarà concordato di volta in volta con le singole Amministrazioni e comunque - salvo diversa indicazione da parte dell'Amministrazione e nel rispetto delle normative vigenti - per un **periodo garantito non inferiore a 1 mese dalla fine delle attività**. Tutte le informazioni, compresi i report tecnici, saranno condivise con le Amministrazioni secondo modalità e protocolli atti a garantire la confidenzialità e integrità delle informazioni scambiate (con impiego ad esempio di tecniche di firma digitale e crittografia dei dati), secondo modalità concordate durante la fase 1 di "Planning e Preparation", anche a salvaguardia dei requisiti dettati dal GDPR.

**Approccio operativo.** Il RTI si impegna ad erogare le attività in ambito nel rispetto dei requisiti tecnico-funzionali specificati nel CTS. Si sottolinea che le attività operative riportate di seguito offrono una sintesi di alto livello delle attività che saranno svolte dal team: ● **Planning and Preparation:** a seguito della richiesta dell'Amministrazione per esecuzione di PT sarà pianificato ed eseguito un Kick Off meeting dove verranno discussi gli aspetti preliminari per l'esecuzione delle attività, con particolare focus su perimetro dell'attività (target in scope e criticità degli stessi), vincoli operativi e regole d'ingaggio. Inoltre, saranno concordate le metriche di valutazione/prioritizzazione delle vulnerabilità (CVSS, Vulnerability Priority Rating, Asset Criticality Rating, Change Criticality Rating) e sarà fornita una proposta di pianificazione delle attività comprensiva di date e orari di inizio e fine. La presente fase infine prevede l'installazione e/o la configurazione degli strumenti hardware e software necessari per l'esecuzione delle analisi. All'avvio delle attività il RTI, sulla base della propria esperienza e del contesto di riferimento in cui saranno svolte le analisi di sicurezza, proporrà gli strumenti di analisi più adatti per l'esecuzione dei PT; tale lista di strumenti (open-source, proprietari e/o di mercato) potrà essere rivista, se strettamente opportuno, con l'Amministrazione e adattata sulla base delle esigenze specifiche e della complessità dell'Amministrazione stessa. ● **Information Gathering:** sarà effettuata l'acquisizione delle informazioni esposte dagli applicativi e dai sistemi che li ospitano al fine di contestualizzare gli attacchi da portare a termine. Tipicamente nel corso di questa fase si procede a: ▪ Identificare e classificare i target in domini di analisi in base alle informazioni enumerate o dedotte anche attraverso attività di Intelligence (fonti OSINT); ▪ Identificare i servizi attraverso le informazioni acquisite precedentemente con l'obiettivo di disporre del maggior numero di elementi riguardo all'architettura ed elementi dell'infrastruttura del servizio ed ai software impiegati; ▪ Identificare i vettori d'attacco sfruttabili per il sistema. La corretta identificazione dei vettori d'attacco è funzionale sia al PT che alla identificazione delle contromisure; ▪ Ricerca potenziali vulnerabilità specifiche per la tipologia di target attraverso fonti di Intelligence. ● **Service scanning:** in questa fase sarà effettuata una scansione automatica delle vulnerabilità. I risultati saranno revisionati manualmente per individuare i servizi su cui effettuare attacchi mirati e contestualmente si procederà all'eventuale personalizzazione degli exploit necessari allo sfruttamento delle vulnerabilità. ● **Exploitation:** in base alla tipologia di PT (Infrastrutturale, Applicativo e su Dispositivi), saranno eseguiti una serie di attacchi finalizzati allo sfruttamento delle possibili vulnerabilità identificate. In questa fase potranno emergere anche ulteriori vulnerabilità non note o ulteriori rispetto a quelle identificate durante la fase di Service Scanning. **CAUTELE ADOTTATE NELLA FASE DI EXPLOITATION:** Il RTI adotterà le seguenti **misure e accorgimenti operativi al fine di evitare il sovraccarico e/o indisponibilità dei target oggetto di test:** ● esecuzione ove applicabile dei test in **ambienti di pre-produzione o Staging** escludendo impatti sugli ambienti di esercizio per limitare indisponibilità e/o accesso ai dati di produzione che potrebbero determinare impatti in termini di GDPR ● **esecuzione fuori dall'orario lavorativo** ● esclusione di **impiego di tecniche di Denial of Service** ● condivisione e **richiesta preventiva di autorizzazione** da parte dell'Amministrazione per procedere all'effettivo Exploiting di vulnerabilità che possano determinare impatti critici sui Target oggetto di test ● **impostazione conservativa degli strumenti automatici** al fine di ridurre eventuali congestioni di rete o sovraccarico/indisponibilità dei sistemi. Per tutte le vulnerabilità con classificazione alta e critica, salvo diversi accordi, sarà cura del team operativo la segnalazione tempestiva ai referenti designati, nel rispetto dei vincoli di confidenzialità e integrità del dato. Analoga prassi sarà adottata se le vulnerabilità riscontrate dovessero riguardare dati personali con impatti GDPR ● **Post-Exploitation:** una volta ottenuto l'accesso al sistema target si proseguirà all'individuazione ed acquisizione delle informazioni reperibili localmente al fine di porre le basi per l'elevazione dei privilegi o l'attacco di sistemi adiacenti (Privilege Escalation, Discovery, Credential Access, Lateral Movement). Nello specifico: ▪ Identificare le vulnerabilità locali: il sistema viene analizzato dall'interno per individuare le vulnerabilità locali note o le configurazioni errate che consentono l'elevazione dei privilegi; ▪ Identificare i file/dati interessanti: vengono cercati sul sistema file utili (es. backup, dump del database, script, password hardcoded) per elevare i privilegi, impersonare altri utenti ed acquisire dati confidenziali; ▪ Identificare le relazioni di fiducia: vengono individuate le relazioni di fiducia con i sistemi o componenti adiacenti al fine di portare a termine degli attacchi strutturati sull'intero insieme dei sistemi oggetto di verifica; ▪ Privilege escalation: vengono portati a termine attacchi per elevare il livello di privilegi sul sistema/applicazione attaccata; ▪ Rimozione strumenti di attacco: in questa fase viene eseguita una rimozione di tutti gli strumenti utilizzati nel corso delle attività legate al Penetration Test; ▪ Proof of Concept: durante tale fase per le vulnerabilità alte e critiche potranno essere dimostrate le limitazioni di sicurezza e le vulnerabilità identificate attraverso lo sviluppo di "Proof of Concept". Nel caso in cui durante la fase di Exploiting, il tester identifichi l'**evidenza di un attacco o compromissione del target in corso o già avvenuta**, si procederà con **tempestiva notifica** all'Amministrazione e l'attività sarà interrotta. Questo approccio evita il potenziale inquinamento di eventuali evidenze presenti sui target, **salvaguardando un potenziale intervento di analisi forense** ● **Reporting:** concluse le attività di analisi sarà predisposta la reportistica dettagliata di quanto effettuato per fornire indicazioni sull'andamento dello stato di sicurezza dei target. La reportistica, prodotta e consegnata al termine di ogni sessione di PT, prevedrà un documento di executive summary e un technical report.

**8.1.1 STRUMENTI E SOLUZIONI TECNOLOGICHE.** Di seguito sono riportati i principali strumenti/soluzioni tecnologiche che saranno utilizzati per l'erogazione del servizio. Gli strumenti/tool di analisi riportati di seguito sono da intendersi a titolo non esaustivo. Nel corso delle attività, anche in considerazione dell'evoluzione delle minacce cyber, dell'utilizzo di tecnologie specifiche da parte dell'Amministrazione nonché dell'evoluzione del processo tecnologico potranno essere utilizzati ulteriori strumenti al fine di garantire un livello di qualità elevato nel corso delle attività.

Ambito di utilizzo	Principali strumenti
PT Infrastrutturale	● <b>Open Source:</b> nmap, netdiscovery, dnsrecon, dig, metasploit, netcat, masscan,scapy,hping, CrackMapExec, Air-Ng tools, Wifite, Airededdon, Wireshark; ● <b>Di Mercato:</b> Acrylic WIFI, Hak5 Wifi (HW e SW), Nessus
PT Applicativo	● <b>Open Source:</b> Objection, Frida,Apktool, Dex2jar, Hopper, Drozer, MobSF, Clang Static Analyzer, Andrubis, Flawfinder, ApkAnalyser, Androwarn, Ghidra, Radare; ● <b>Di Mercato:</b> Nessus, Burp Proxy Professional

Ambito di utilizzo	Principali strumenti
PT Device IOT	● <b>Open Source:</b> Burp Proxy Professional, Blue Scanner, Blue Sniff, BlueBugger, BTBrowser, BTCrawler, BlueSnarfing, ZigDiggity; ● <b>Di Mercato:</b> HackRF, Proxmark
Red Team	● <b>Open Source:</b> Social Engineering Toolkit (SET), Gophish, Invoke-Obfuscation, Veil Framework, Empire Project, DNSExfiltrator, Cloakify Factory; ● <b>Di Mercato:</b> Cobalt Strike, Metasploit Pro

**8.2 PROPOSTA DI DELIVERABLE DOCUMENTALI.** A seguito delle attività svolte in ambito Penetration Test sono **proposti i seguenti deliverable documentali** necessaria a fornire all'Amministrazione una visione di alto livello, nonché tecnica, dello stato di sicurezza dei target oggetto delle analisi:

Deliverable	Contenuti esemplificativi
PT Executive Summary	Report direzionale, con vista Executive, pensato per fornire una visione concreta al Management dello stato di sicurezza del patrimonio informativo. Tale report includerà un riepilogo generale delle attività eseguite e sintetizzerà i risultati ottenuti. Nello specifico: ● Sintesi delle attività svolte e dei sistemi sottoposti ad analisi, con informazioni relative alla loro criticità per l'Amministrazione nonché di eventuali impatti normativi come GDPR; ● Sintesi dei risultati con indicazione dei sistemi vulnerabili, aggregati per tipologia di vulnerabilità e livello di criticità (in termini qualitativi, ovvero il livello di vulnerabilità complessivo - alto, medio, basso – e quantitativo numero di vulnerabilità totali, critiche e elevate). Saranno inoltre evidenziati gli impatti qualitativi (secondo i livelli alto, medio e basso in coerenza con quanto definito dal CVSSv.3), in caso di ipotetico sfruttamento delle vulnerabilità da parte di un attaccante Cyber, in termini di perdita di confidenzialità, integrità e disponibilità dei dati dell'Amministrazione e le principali cause che portano alla presenza e potenziale sfruttamento della vulnerabilità sui target in ambito. ● Sintesi delle principali azioni di rimedio – Classificate/prioritizzate in termini qualitativi (esecuzione nel breve, medio e lungo termine) definite a mitigazione delle vulnerabilità e rappresentazione del remediation plan con evidenza delle azioni prioritarie e delle tempistiche necessarie per l'implementazione delle stesse.
PT Technical Report	Documento tecnico contenente un'analisi dettagliata e completa del livello di sicurezza, insieme a tutte le informazioni sulle vulnerabilità riscontrate, sulle modalità di sfruttamento e relative azioni per mitigare e, ove possibile, per eliminare tali vulnerabilità. Il Technical Report è formato da resoconti analitici e grafici e contiene i seguenti elementi principali: ● Descrizione di dettaglio dei test di sicurezza eseguiti sui target in ambito (on premises - on cloud); ● La lista di tutte le vulnerabilità riscontrate con indicazione di: nome della vulnerabilità sulla base del CVE (Common Vulnerabilities and Exposures), livello di severità in base alla probabilità di sfruttamento (alto, medio, basso) ed all'impatto legato allo sfruttamento della vulnerabilità (alto, medio, basso per Riservatezza, Integrità e Disponibilità - RID), dettagli tecnici sulla vulnerabilità rilevata ed evidenze documentali (con eventuale supporto di immagini e tabelle) delle attività svolte (comandi eseguiti e risposte dei sistemi). <b>Le informazioni dimensionali</b> per la valutazione delle vulnerabilità e delle relative remediation, sono basate sul sistema di scoring delle vulnerabilità CVSS e sono principalmente le seguenti: <b>vettore di attacco, complessità di attacco, privilegi richiesti, tipologia di interazione dell'utente, possibilità di propagazione, impatti su confidenzialità, integrità e disponibilità</b> . Ciascuna delle dimensioni citate sono valorizzate su una scala dimensionale da 1 a 10, con una sintesi finale di rischio che può assumere i <b>seguenti valori qualitativi</b> : critico, alto, medio o basso.
PT Remediation Plan	<b>Remediation plan</b> comprensivo delle iniziative tecniche da pianificare e svolgere per la mitigazione/risoluzione delle vulnerabilità identificate. Per ogni azione di rimedio sono fornite le seguenti <b>informazioni dimensionali</b> di dettaglio: attività da svolgere per la risoluzione delle vulnerabilità, complessità richiesta, nonché tempistiche dell'Amministrazione per l'esecuzione della stessa. Ciascuna delle dimensioni citate è valorizzata secondo le seguenti <b>informazioni qualitative</b> : tipologia di remediation (es: <i>R1-risoluzione completa</i> con azione da implementare, <i>R2-soluzione alternativa/compensativa/workaround</i> ), complessità per la risoluzione tecnica della vulnerabilità ( <i>C1-molto alto</i> , <i>C2-alto</i> , <i>C3-medio</i> o <i>C4-basso</i> ), tempistiche di risoluzione stimate ( <i>T1-ore</i> , <i>T2-giorni</i> , <i>T3-settimane</i> o <i>T4-mesi</i> con relativa proposta di pianificazione). Tali parametri sono determinati sulla base della collaborazione con i principali team operativi dell'Amministrazione impattati dalla vulnerabilità riscontrata e dall'azione di rimedio definita per la risoluzione. La determinazione di <b>Priorità nell'applicazione delle azioni di rimedio</b> è infine determinata dalla combinazione delle informazioni qualitative descritte e la <b>rischiosità della vulnerabilità</b> . Il parametro di Priorità risultante è espresso in termini di <i>P1-Critica</i> , <i>P2-Alta</i> , <i>P3-Media</i> o <i>P4-Bassa</i> .

**8.3 TEAM DI LAVORO.** Il team ottimale rispetterà i requisiti specificati nel CTS a cui si aggiungeranno i requisiti migliorativi sintetizzati di seguito.

Profilo	Requisito migliorativo generale
Security Principal	● Nel caso di esecuzione di PT di tipo mobile nel team sarà inserita almeno una figura con in possesso la certificazione <b>eMAPT</b> ● Nel caso di esecuzione di PT di tipo infrastrutturale nel team sarà inserita almeno una figura in possesso di almeno una delle seguenti certificazioni: <b>eCPPT, GPEN, OSCP, eCPTX, OSWP,eCXD,eCTHP,CRTP,eIPT</b> ● Nel caso di esecuzione di PT di tipo applicativo nel team sarà inserita almeno una figura con in di almeno una delle seguenti certificazioni: <b>OSWE, eWPTx, eCTHP, CRTP, eIPT</b>
Senior Penetration Tester	
Junior Penetration Tester	
Forensic Expert	

## 9 PROPOSTA PROGETTUALE PER IL SERVIZIO "COMPLIANCE NORMATIVA"

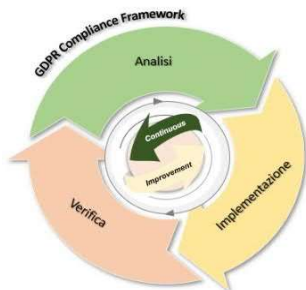
Il servizio di Compliance normativa prevede la definizione di un **Sistema di gestione della Privacy** in grado di governare **in un'ottica di lungo periodo** tutti gli adempimenti GDPR impattanti sui sistemi IT. Il RTI si impegna ad erogare le attività in ambito nel rispetto dei requisiti tecnico-funzionali specificati nel CTS, facendo affidamento sugli elementi distintivi elencati di seguito:

**1. Multidisciplinarietà delle competenze (IT, legali, operative e organizzative) integrate in team strutturati**, dimostrata nel corso di **oltre 500 esperienze progettuali realizzate a livello nazionale negli ultimi 4 anni per più di 150 clienti**. Utilizzo del **GDPR Compliance Framework (GDPR CF)**, strumento per l'automazione ed il governo dei processi, che include la metodologia per lo svolgimento delle attività, modelli (differenziati per tipologia e complessità delle

amministrazioni considerate), processi, questionari, baseline di requisiti, strumenti automatizzati, in grado efficientare le attività progettuali **3. Costante aggiornamento normativo realizzato attraverso l'Osservatorio Privacy** del RTI che si avvale anche della **collaborazione con l'Università Statale di Milano, POLIMI, Università Luiss ed associazioni in ambito privacy e security** come IAPP e ISACA, dimostrato anche dalle molteplici **pubblicazioni** (oltre 20) relative ai servizi di compliance GDPR **4. DRA ed EYA si possono avvalere della collaborazione dei propri Studi Legali Associati. Il team legale italiano EY è stato insignito, a conferma delle capacità e competenza in ambito privacy, per il quarto anno consecutivo del Corporate Intl Magazine Global Award e del Global Law Experts (GLE), nella categoria "Data Privacy Law" in Italia, premio di rilevanza internazionale.**

## 9.1 MODALITA' DI ESECUZIONE DEL SERVIZIO, AMBITI DI INTERVENTO, MODELLO ORGANIZZATIVO E STRUMENTI.

### 9.1.1 MODALITA' DI ESECUZIONE DEL SERVIZIO E AMBITI DI INTERVENTO



Il Sistema di gestione della Privacy ha necessità di essere disegnato, analizzato, implementato, monitorato e continuamente migliorato in un'ottica anche di lungo periodo, al fine di trasformare la privacy in un **fattore abilitante** per il trattamento dei dati da parte dell'Amministrazione e garantire agli interessati (es. cittadini, utenti, dipendenti dell'Amministrazione) la protezione dei dati personali. A tale scopo, il RTI utilizzerà, per guidare lo svolgimento delle attività, il **GDPR Compliance Framework (GDPR CF)**. Tale strumento propone una metodologia per la definizione e mantenimento del sistema privacy ed è caratterizzato da un ciclo di 4 fasi: a) Analisi; b) Implementazione; c) Verifica; d) Continuous Improvement. Quest'ultima fase è abilitata dal **Privacy Maturity Model (PMM)**, ovvero uno strumento in grado di intercettare nel continuo, i punti di forza e di miglioramento del Sistema di gestione della privacy esprimendo lo stato di

maturità e identificando in modo dinamico le aree di intervento. L'utilizzo del GDPR CF, oltre a mettere a disposizione un **set esaustivo di strumenti automatici**, potrà, in funzione delle esigenze progettuali, essere supportato da un **prodotto software integrato che consente di gestire il Sistema Privacy in modalità condivisa e collaborativa tra tutti i soggetti interessati** (es. DPO, Privacy Officer, IT, Sicurezza, Risorse Umane, Acquisti). In entrambi i casi saranno garantite tutte le funzionalità sotto descritte. Con particolare riferimento agli strumenti di analisi e template, in analogia al servizio di Security strategy, il framework prevede **modelli differenziati per tipologia e complessità delle amministrazioni considerate** (in tal modo, considerando la completa copertura dei requisiti privacy, i template/checklist saranno più o meno articolati a seconda che si consideri una grande o una piccola amministrazione).

**Legenda:** □ funzionalità automatizzata. **a) Analisi:** La fase di analisi prevede lo svolgimento di un **assessment** (□) per verificare lo stato di conformità alla normativa applicabile da parte delle Amministrazioni al fine di comprendere le aree maggiormente a rischio e identificare gli eventuali interventi di rimedio necessari per garantire conformità e allo stesso tempo automatizzare i processi privacy. A beneficio di tale attività e delle successive, il RTI potrà avvalersi di un **"Osservatorio Privacy"** il cui scopo è quello di recepire ed analizzare tempestivamente le evoluzioni normative (normativa, regolamenti, standard, provvedimenti del Garante Privacy). All'avvio delle attività di assessment il RTI individuerà e formalizzerà un Compendio contenente norme, regole e principi rilevanti per l'Amministrazione (es. provvedimenti del Garante Privacy, LLGG in tema di FSE e DS, opinion del EDPB). Sulla base della tipologia di amministrazione ed in particolare della tipologia di dati trattati, il GDPR CF consentirà di definire una **GDPR Requirements Checklist** contenente i requisiti GDPR applicabili ai diversi macro ambiti (es. struttura del registro dei trattamenti, misure di sicurezza in funzione dei livelli di rischio, gestione delle richieste degli interessati e notifiche dei data breach). Il **GDPR Requirements Checklist** è uno strumento parametrizzabile che consente di ottenere check-list di analisi (basati su standard quali ISO27701, linee guida ICO, ENISA, CNIL) sulla base della tipologia dell'amministrazione e dei dati trattati e attraverso domande specifiche e punteggi assegnati automaticamente ad ogni risposta (la maggior parte a risposta chiusa), la definizione dell'attuale livello di conformità e la rilevazione dei Gap. Sulla scorta di tale strumento, il RTI ● raccoglierà ed analizzerà la documentazione disponibile in ambito (ad esempio, ove esistenti, politiche e procedure, registro dei trattamenti, classificazione dei dati, esiti della valutazione dei rischi e di verifiche/audit); ● svolgerà i necessari approfondimenti tramite intervista con i referenti dell'Amministrazione, ad esempio DPO, referenti IT e Sicurezza, HR, principali outsource; ● identificherà il perimetro dei sistemi IT contenenti dati personali, le misure tecniche di sicurezza e le soluzioni tecnologiche in essere, nonché i sistemi che raccolgono i consensi al trattamento dati di soggetti esterni ed interni; ● predisporrà e compilerà le **schede per il censimento dei trattamenti** e sulla base di queste provvederà alla redazione/aggiornamento del registro dei trattamenti attraverso l'utilizzo del **Record of Processing Activities (ROPA) Template** che permettono di ridurre, fino ad eliminare, scambi di email e garantire una governance centrale dei trattamenti; ● laddove richiesto effettuerà, propedeuticamente alla compilazione del registro, la discovery automatica delle informazioni strutturate e destrutturate presenti sugli asset informativi (Hawk Discovery); ● classificherà i dati attraverso la **definizione del livello di criticità** delle tipologie di dati trattati (es.: dato sanitario) dall'Amministrazione (**Data Classification**). Sulla scorta delle informazioni raccolte, in particolare sulla natura dei trattamenti, il RTI personalizzerà la GDPR Requirements Checklist ed eseguirà una Gap Analysis dei presidi esistenti per l'individuazione dell'attuale livello di conformità. A titolo di esempio e con riferimento alle **misure tecniche IT/Sicurezza** saranno analizzate: le modalità di accesso dei dati da remoto, le **modalità tecniche di attuazione delle richieste da parte degli interessati di cancellazione e/o modifica e/o accesso**, la nomina e verifica degli amministratori di sistema, la gestione dei log, la cifratura delle basi dati, ecc. Il risultato di tale attività sarà un **Report di Compliance** che evidenzierà i gap per una piena conformità al Regolamento. Tale Report includerà la proposta del **Piano degli interventi** che include gli interventi utili a mitigare il rischio di non conformità, espressi in termini di attività previste e approccio operativo, risultati attesi, roadmap di implementazione e stime dei costi di realizzazione. Il piano prevederà interventi di tipo organizzativo, di processo o tecnologico ed in particolare, l'adozione di **tecnologie IT/Sicurezza** utili al miglioramento della protezione dei dati personali (es. dispositivi per gestire i cookies, sistemi di encryption/mascheramento, modalità sicure di autenticazione – es. strong authentication). Report e Piano saranno condivisi tramite specifici workshop con l'Amministrazione e, ove possibile, in sinergia con le attività di supporto agli stakeholder delle strutture di vertice dell'Amministrazione proposte nel servizio di Security Strategy (§ 4.1.1.3).

**b) Implementazione** (□): Tale fase consentirà di indirizzare le azioni di rimedio emerse a seguito dell'Assessment ed incluse nel Piano degli interventi - o già previste dai piani di conformità dell'Amministrazione. Allo scopo di **massimizzare l'efficacia degli interventi e la logica del riuso**, le attività di implementazione sono eseguite secondo un modello operativo che prevede la messa a disposizione di template consolidati per le componenti del framework documentale (es. politiche, procedure, metodologie, nomine a responsabile, informative, data processing agreement, materiale formativo) che saranno condivisi con



l'Amministrazione e personalizzati sulla base delle specifiche necessità. Per tali attività l'approccio proposto sarà: ● comprensione del contesto e raccolta delle informazioni per quanto non già emerso in fase di Analisi; ● predisposizione di una proposta dei componenti del framework documentale a partire da modelli coerenti per tipologia e complessità dell'Amministrazione, customizzati sulla base delle informazioni raccolte; ● condivisione con l'Amministrazione ● fine tuning e finalizzazione. Per tale fase si prevedono, a titolo esemplificativo e non esaustivo, le seguenti attività (per ciascuna di esse sono citate le funzionalità utilizzate a supporto): ● Definizione e/o aggiornamento del **modello organizzativo privacy**, sulla base di modelli coerenti per tipologia e complessità dell'Amministrazione, ivi inclusi ruoli (es. Amministratori di Sistema), responsabilità e flussi informativi anche verso le altre figure previste nel modello quali Titolare, DPO ed Incaricati. Allo scopo il RTI popolerà e manterrà un Repository dei modelli organizzativi per tipologia di Amministrazione (**GDPR Benchmark Repository**) ● Definizione di processo, procedure e politica di **data retention e deletion** comprensivi delle regole da applicare per ogni sistema (**Data Retention Matrix** - strumento per la determinazione delle tempistiche massime di conservazione dei dati in funzione della loro tipologia - per la determinazione delle tempistiche massime di conservazione dei dati in funzione della loro tipologia). Tali regole consentiranno all'Amministrazione di implementare **azioni automatiche** (es. script, query realizzate su dati strutturati dai DBA) **per cancellare, anonimizzare o pseudonimizzare** i dati; ● Definizione di processo e procedure per la **gestione delle richieste dei soggetti interessati** nonché dei modelli di risposta alle richieste (**Moduli DSR**) con i relativi strumenti/pratiche IT/Sicurezza (es. individuazione dei dati, portabilità, cancellazione) a supporto; ● Definizione del **processo di Privacy by Design**, incluse le misure tecniche IT/Sicurezza (es. sistemi di data loss prevention, tecniche di cifratura, gestione e monitoraggio degli accessi amministrativi, tracciamento degli eventi/log) ed organizzative necessarie per assicurare che siano trattati, fin dalla progettazione e per impostazione predefinita, solo i dati necessari per ogni specifica finalità di trattamento nel rispetto del principio di minimizzazione (**Privacy by Design Checklist – PbDC**); ● Definizione di processi, modelli standard e adozione di uno strumento (**Notification Criteria workflow**) per la valutazione dell'impatto di un eventuale **Data Breach** e la gestione dell'eventuale notifica all'Autorità Garante o la comunicazione ai soggetti interessati. Si noti che, laddove il data breach fosse di natura informatica, il processo sarà integrato con quanto definito per il servizio di gestione degli incidenti informatici (§7.1). Il **Notification Criteria workflow** è basato su metodologie approvate dalle Autorità di Controllo, contiene i criteri (es. numero di interessati coinvolti, tipo di dati violati, ecc) da applicare per la valutazione dell'impatto di un eventuale breach; ● **Definizione di una metodologia di analisi dei rischi privacy** che consenta di valutare la rischiosità intrinseca dei trattamenti dell'Amministrazione e di avviare anche l'eventuale processo di analisi degli impatti (DPIA) per i trattamenti a rischio elevato (**Risk Analysis & DPIA** - per l'esecuzione dell'analisi dei rischi o della DPIA in maniera guidata, con il supporto di workflow autorizzativi e uso di algoritmi che permettano una determinazione automatica dell'impatto e rischio residuo); ● Elaborazione di un piano di comunicazione e formazione del personale dell'Amministrazione; ● Preparazione di **corsi in modalità e-learning** oppure erogazione di **sessioni formative in aula/remoto** sui requisiti previsti dal GDPR e rilevanti per l'Amministrazione, comprensivi di test di valutazione delle competenze acquisite e richiami periodici di aggiornamento; **simulazioni di specifici processi** descritti dalle politiche e procedure prodotte, con il coinvolgimento del personale addetto (es. simulazioni di data breach; simulazione di **ispezione da parte dell'Autorità Garante** con il supporto anche di spazi innovativi, come il **Wavespace di EYA** e il **GreenHouse di DRA**); invio periodico di **Privacy Highlights**, ovvero newsletter con le principali novità legislative e avvenimenti privacy.

**c) Verifica (☐):** tale fase consente di misurare l'effettiva implementazione dei requisiti normativi a cui è soggetta l'Amministrazione, valutare il rischio derivante dai gap ed il livello di maturità raggiunto, proponendo eventuali punti di miglioramento, attraverso piani di azione costantemente monitorati. Tale fase prevederà le seguenti attività: ● predisposizione e condivisione di un piano delle verifiche; ● affinamento di dettaglio e finalizzazione del piano; ● esecuzione dell'attività di verifica; ● condivisione preliminare dei risultati con i referenti delle attività oggetto di verifica; ● predisposizione di un report di sintesi e di dettaglio delle verifiche, ciascuno dei quali prevederà: ▪ le osservazioni effettuate; ▪ gap, i punti di miglioramento o le aree di forza individuate; ▪ la proposta di action plan; ▪ l'azione condivisa con l'Amministrazione; ▪ presentazione finale dei risultati. Per tale fase il RTI propone l'elaborazione di un **piano periodico di verifiche di conformità** che potrà includere, a titolo esemplificativo e non esaustivo, le seguenti tipologie di verifica: ● **Audit verticale sui requisiti GDPR**: verifica, attraverso l'uso della **GDPR Audit Checklist** (strumento parametrizzabile per tipologia di amministrazione ed ambito di verifica), dell'adeguata implementazione dei processi e dei controlli definiti nella fase implementativa, rispetto ai requisiti privacy applicabili ● **Audit periodici sui responsabili esterni del trattamento** tramite la determinazione dei criteri di selezione delle terze parti e la definizione della modalità di verifica (self-assessment, documentale, on-site) anche attraverso il **Third Party Risk Assessment**; ● **Audit sui consensi**, che, sulla base dei sistemi IT che raccolgono consensi, sia interni che esterni, prevede la verifica dell'esistenza di documentazione/evidenze del rilascio del consenso informato, l'analisi delle caratteristiche/configurazioni dei software adibiti alla gestione del consenso; individuazione automatica dei trattamenti basati sul consenso ● **Stress Test** con simulazioni di ispezioni da parte dell'Autorità Garante Privacy e simulazione di esercizio dei diritti degli interessati. Sulla base degli esiti del piano periodico di verifiche, il RTI supporterà l'Amministrazione nell'elaborazione della reportistica relativa agli esiti delle verifiche di compliance (**Rapporti di compliance**).

**d) Continuous Improvement:** Al fine di trasformare la privacy **da adempimento di legge ad abilitatore "mandatorio"** e cogliere tempestivamente i rischi normativi/sanzionatori/IT, si prevede l'adozione del **PMIM** (o in alternativa il Data Protection Maturity Self-Assessment Model rilasciato dal CNIL). Tali modelli permettono di misurare in modo continuativo e dinamico lo stato di maturità dei processi privacy, di business e IT in conformità alla normativa applicabile e quindi consentire sia di **monitorare** il piano complessivo degli interventi, sia di cogliere **aree di miglioramento** e/o **automazione di alcuni processi** in un'ottica di *continuous improvement*. Il PMIM non sostituisce, ma integra e rafforza le verifiche periodiche, divenendo uno strumento utile a supporto dell'Accountability del Titolare, attraverso la definizione di indicatori (**KPI** e **KRI**) alimentabili in maniera semi-automatica e continua, così da offrire all'Amministrazione una visione di conformità e maturità privacy misurabile e completa in ogni momento. Lo strumento permette quindi di accelerare e rendere proattive le **attività di rimedio**, rendendole integrate **by design nei processi di business**. A titolo esemplificativo nel PMIM saranno rappresentati, attraverso un cruscotto di indicatori (es. tempi di evasione delle richieste interessati, trattamenti ad alto rischio con DPIA eseguita, data protection agreement sottoscritti), i livelli di maturità dell'Amministrazione rispetto ai requisiti privacy con un collegamento ai rischi che il livello di maturità identificato può comportare

**9.1.1.1 DELIVERABLE** - Si propone di seguito un elenco non esaustivo dei deliverable che saranno predisposti:

Deliverable	Contenuti esemplificativi
<b>Rapporti di compliance</b>	I dettagli sulla struttura del template sono presenti all'interno della sezione §9.3.

<b>Scheda censimento e registri dei trattamenti</b>	Registri dei trattamenti (in titolarità e responsabilità), derivanti dalla fase di implementazione, corredati da apposite schede/questionari automatizzati per la compilazione/aggiornamento.
<b>Set documentale in ambito privacy</b>	Set documentale, derivante dalla fase di implementazione, composto da policy, procedure operative, manuali, template di misure di sicurezza ed altra eventuale documentazione (es. la procedura di gestione dei data breach, metodologia di DPIA o procedura di Privacy by Design).
<b>Maturity Dashboard</b>	Dashboard, derivante dalla fase di continuous improvement, contenente indicatori, anche autoalimentati, che mostrano in modo dinamico lo stato di maturità della privacy evidenziando aree su cui è necessario intervenire.

**9.1.2 MODELLO ORGANIZZATIVO PROPOSTO.** Il modello prevederà un team di progetto guidato da un Project Manager (Security Principal) che avrà lo scopo di definire, in accordo con l'Amministrazione, le tempistiche e le milestone progettuali. Tale risorsa coordinerà lo svolgimento delle differenti attività, assicurando in particolar modo che le competenze del Data Protection Specialist siano pienamente integrate nello svolgimento delle attività e che possano essere di indirizzo allo svolgimento delle attività svolte dalle figure con una competenza maggiormente tecnologica. Il Data Protection Specialist a tale proposito sarà maggiormente coinvolto nelle fasi di analisi ed implementazione e sarà supportato dalla figura del Senior e Junior Information Security e Consultant nelle attività più strettamente legate ad aspetti di sicurezza quali il supporto nella valutazione delle misure di sicurezza tecniche, nelle procedure di supporto della garanzia di confidenzialità, integrità e disponibilità dei dati. Specialmente nella fase di verifica sarà coinvolto il Senior Security Audit che, sempre guidato dal Project Manager, sarà la figura preposta all'esecuzione delle verifiche sui sistemi informativi. Per tali verifiche, vista l'ampiezza del perimetro, il team sarà inoltre integrato con le competenze più verticali del Data Protection Specialist. **Ove necessario il RTI potrà accedere a competenze e risorse ulteriori disponibili nei relativi Studi Legali Associati per la valutazione e l'interpretazione dei risvolti normativi delle attività svolte.**

**9.1.3 STRUMENTI E SOLUZIONI TECNOLOGICHE.** Nel corso delle attività di Compliance Normativa, il RTI utilizzerà strumenti e soluzioni tecnologiche al fine di efficientare, automatizzare e rendere più efficaci ed accelerare le fasi di analisi, implementazione, verifica e continuous improvement. In particolare:

Ambito di utilizzo	Principali strumenti
Analisi/ Implementazione/ Verifica	<p>● <b>GDPR CF – Compliance Framework</b> Lo strumento <b>proprietario</b> include a titolo esemplificativo e non esaustivo le seguenti funzionalità (<u>Analisi</u>) GDPR Requirement Checklist; ROPA Template; Data Classification (<u>Implementazione</u>) Privacy by Design Checklist; Risk Analysis &amp; DPIA; Data Retention Matrix; Il Notification Criteria Workflow; Moduli DSR; (<u>Verifica</u>) GDPR Audit Checklist; Third Party Risk Assessment.</p> <p>● <b>DPPM - Data Protection Platform Management</b> – strumento <b>proprietario</b> che supporta le varie attività del Sistema di gestione privacy come ad esempio: la manutenzione del registro dei trattamenti attraverso l'uso di una console centralizzata di monitoraggio e un invio di link per la review dei dati presenti sul registro dei trattamenti, la gestione dei breach attraverso modelli definiti sulla base dei requisiti espressi dal Garante e che consentono in modo "automatico" di comprendere la necessità o meno di segnalare il breach; le richieste degli interessati permettendo di censire le stesse in modo ordinato e facilitando il rispetto dei tempi di risposta. Si sottolinea che il RTI potrà svolgere le attività anche utilizzando strumenti di cui l'amministrazione si è già dotata.</p>
Analisi Implementazione	<p>● <b>Hawk Discovery</b> strumento <b>proprietario</b> utilizzato per le attività di data discovery e data classification automatizzate.</p> <p>● <b>GDPR Benchmark Repository</b>, archivio documentale contenente modelli organizzativi e modelli di policy e procedure.</p>
Continuous Improvement	<b>Privacy Maturity Model (PMM)</b> o <b>Data Protection Maturity Self-Assessment Model</b> del CNIL, strumenti per la misurazione del livello di maturità raggiunto dall'Amministrazione.

**9.2 PROPOSTA DI RAPPORTO DI COMPLIANCE** I rapporti di compliance sono dei report che inducono al loro interno la **valutazione sullo stato di conformità privacy** rispetto alle analisi e/o verifiche effettuate. In funzione dell'ambito di analisi, i rapporti considereranno i **criteri di verifica** applicabili a tutto il Sistema Privacy o a specifici ambiti di analisi (es. misure di sicurezza tecniche IT/Sicurezza, data retention, cookies, consensi). I criteri di verifica misurano l'aderenza ai requisiti Privacy, l'esposizione al rischio sanzionatorio, l'efficacia e la maturità del Sistema Privacy. Fra i criteri di verifica, saranno considerati, a titolo esemplificativo e non esaustivo, gli aspetti inerenti la completezza del registro dei trattamenti, la completezza delle nomine a responsabile, l'esattività delle verifiche delle attività svolte dagli Amministratori di Sistema, l'adeguatezza delle misure IT/Sicurezza in uso. I Rapporti saranno strutturati secondo le seguenti sezioni principali: a) **sintesi, obiettivi, criteri di verifica, perimetro e tempistiche** delle attività svolte; b) **descrizione delle attività**, anche in ottica IT fornendo le informazioni necessarie per le attività di verifica sui sistemi e le relative misure di sicurezza; c) **risultati e raccomandazioni**. A seconda dell'ambito di verifica della compliance, al rapporto saranno allegate checklist compilate, evidenze documentali e procedurali o di configurazioni sistemiche se l'attività fosse di tipo tecnico ed effettuata sui sistemi IT. Ogni rapporto di compliance sarà, in tale sezione, corredato da una scheda di valutazione per la formalizzazione degli esiti dei controlli. La valutazione prevederà a titolo indicativo l'assegnazione di un rating, l'identificazione dei **gap rilevati** che supportano il rating assegnato, l'identificazione delle azioni di rimedio ritenute necessarie per colmare i gap identificati e del livello di priorità delle azioni (da urgente a rinviabile) d) **Piano degli interventi**: piano delle attività, derivante dalla fase di analisi, suddiviso per interventi di tipo documentale, di processo o tecnologici estesi ai macro ambiti di intervento (secondo i contenuti descritti nel paragrafo §4.1). Tali azioni saranno quindi di **input anche per la fase di Continuous Improvement**

**9.3 TEAM DI LAVORO.** Il team ottimale rispetterà i requisiti specificati nel CTS a cui si aggiungeranno i seguenti requisiti migliorativi.

Profilo	Requisito migliorativo Generale	Requisito migliorativo Specifico
Security Principal	Nel team sarà inclusa almeno una risorsa con certificazione <b>CIPP/E o CDPSE</b>	
Data Protection Specialist		
Junior Information Security Consultant		

Senior Information Security Consultant	Possesso della qualifica di <b>Lead Auditor ISO 27001</b> aggiornata all'ultima release, per almeno il <b>70%</b> delle risorse, appartenenti al suddetto profilo professionale, nell'ambito di ciascun contratto esecutivo
Senior Security Auditor	Possesso della qualifica di <b>CISA</b> , per almeno il <b>70%</b> delle risorse, appartenenti al suddetto profilo professionale, nell'ambito di ciascun contratto esecutivo

## 10 PORTALE DELLA FORNITURA

Il *Portale di Fornitura* che il RTI propone per le attività di governance e di gestione dei servizi e delle iniziative previste da Capitolato, nonché per le attività di comunicazione e condivisione delle esperienze maturate dalle PA aderenti all'AQ, è progettato in ottica di semplificazione e ottimizzazione della esperienza utente e, nel rispetto delle regole AgID, prevede interfacce che lo rendono fruibile da qualsiasi device. Particolare attenzione si pone sui temi dell'**usabilità** per permettere a tutti gli interessati di fruire dei contenuti in maniera agevole. **Un mockup esemplificativo è fornito in Allegato 10.A.**

**1.** Il portale si contraddistingue per la presenza di un **sistema di analytics e reporting**, con report e cruscotti grafici già predefiniti e funzionalità di self-reporting, utili alla gestione di grandi quantità di dati o analisi complesse. **2.** Al fine di migliorare e facilitare la **sinergia e il confronto tra le PA** accreditate tramite un **approccio "social"**, sono inclusi nel Portale molteplici **strumenti di collaborazione e comunicazione** nonché strumenti innovativi di marketing e promozione per la PA nei confronti dei cittadini, dei professionisti e delle imprese, utili anche a mettere in risalto i benefici dei servizi dell'AQ. **3.** Utilizzo di **protocolli e standard "aperti"** che garantiscono un ampio **ventaglio di integrazioni** con strumenti e soluzioni di terze parti.

### 10.1 SOLUZIONI TECNOLOGICHE E FUNZIONALITÀ PROPOSTE

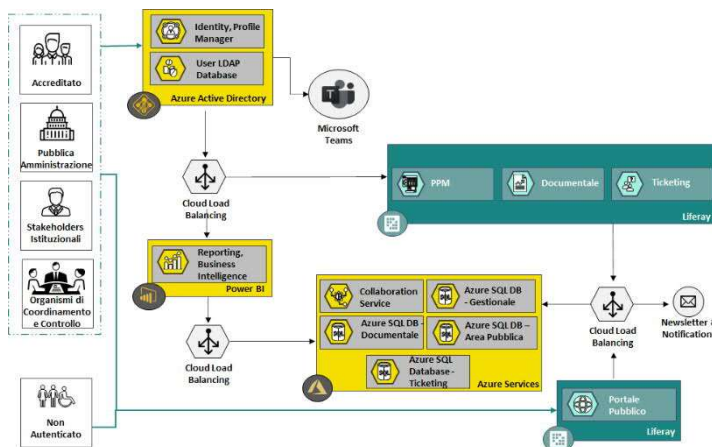
**10.1.1 LA TECNOLOGIA** Le componenti previste per il Portale della Fornitura possono essere raggruppate in 3 tipologie di layer: **●Layer logico:** rappresenta la vista di tutte le funzioni, servizi e processi di business verticali e trasversali per la gestione dell'intera fornitura **●Layer tecnologico:** contiene gli strumenti e piattaforme tecnologiche atte a supportare ed erogare tutte le funzionalità e i servizi del layer logico. Il RTI intende integrare i migliori prodotti di mercato, certificati dai Magic Quadrant di Gartner, per la gestione delle componenti di PPM, Comunicazione, Reporting, Marketing e Customer Satisfaction, quali:

**LIFERAY** è la piattaforma di portali Open Source, leader mondiale, che offre funzionalità di pubblicazione e gestione di contenuti Web. Presenta un'architettura orientata ai servizi e compatibilità con tutte le principali infrastrutture IT; **Microsoft Teams** è una piattaforma di comunicazione unificata che combina in un unico workspace chat di lavoro, email, riunioni video, gestione documenti (compresa la collaborazione istantanea tra più utenti su documenti);

**Power BI** è una piattaforma software di Data Analytics e Business Intelligence (BI) che offre funzionalità di reporting, data integration, OLAP services, information dashboards, data mining e risorse ETL; **hotjar** consente: → di progettare e realizzare survey online su cluster di utenti selezionati, analizzando più variabili in relazione a servizi/processi/percezioni; → di monitorare le conversazioni sia su canali non-owned (forum, blog, pagine Facebook appartenenti ad altre organizzazioni, ecc.) che su canali proprietari (es. portale servizi dell'Amministrazione); → di effettuare sentiment analysis; → la disambiguazione e l'auto-apprendimento basato su un training della piattaforma che consente di migliorare l'accuratezza della selezione fatta in automatico; → il real time tracking e l'analisi delle conversazioni; → sondaggi coinvolgenti sfruttando grafiche accattivanti e icone di gradimento; → di integrarsi con piattaforme per tenere sotto controllo le valutazioni e analizzarne il cambiamento nel tempo.

**●Layer architetturale:** rappresenta la panoramica infrastrutturale del Portale con lo scopo di proporre una soluzione moderna utilizzando le tecnologie più avanzate presenti sul mercato. In particolare, la soluzione consente attraverso un componente di tipo IDaaS (Identity-as-a-Service), inclusa in Office 365, quale Azure Active Directory, di centralizzare il processo di autenticazione in modo sicuro costituendo un meccanismo di Single Sign-On (SSO). L'utente, in funzione del profilo assegnato, viene autorizzato all'accesso a specifiche funzionalità e servizi erogati sia in ambienti SaaS, sia in IaaS ospitati su macchine virtuali Windows. Tali ambienti sono adeguatamente protetti seguendo i principi di progettazione della sicurezza cloud e le best practices dei vendor coinvolti (es: MS Azure), con il fine di garantire la riservatezza, integrità e disponibilità delle informazioni. L'infrastruttura è inoltre protetta da un servizio continuativo di monitoraggio della sicurezza e di gestione degli incidenti informatici focalizzata a rilevare eventuali minacce cyber e coordinare le azioni di mitigazione ed eradicazione. La soluzione, **interamente modulare**, consente al RTI di poter introdurre, durante l'erogazione dei servizi, componenti migliorativi, principalmente *Open Source* nel rispetto delle linee guida AgID, in grado di garantire una costante qualità del servizio. Il portale della fornitura metterà a disposizione un'interfaccia API in grado di integrare, attraverso l'ausilio dei più comuni standard di comunicazione (SOAP e/o REST), eventuali sistemi già in uso dalle PA aderenti all'AQ, come previsto da capitolato, consentendo l'adozione di modalità di lavoro collaborativo e l'uniformità dei flussi di lavorazione. Infine, grazie all'utilizzo di componenti e prodotti di tipo *Cloud-Based*, **verrà garantito un elevato livello di servizio e un'adeguata scalabilità** in funzione degli utenti che usufruiscono dei servizi esposti. Il RTI garantisce il rispetto dei requisiti tecnico-funzionali specificati nel CTS circa le modalità di integrazione degli strumenti con il Portale della Fornitura. **10.1.2 LE FUNZIONALITÀ**

Il Portale proposto si compone di diverse componenti logiche, di business e tecnologiche supportate da appropriate misure per garantire la sicurezza e la protezione dei dati. Il Portale si rivolge a una molteplicità di attori, ciascuno con differente visione e scopo di fruizione. Per questo motivo a ogni profilo di utenza sono dedicate specifiche Aree, funzionalità e strumenti. Le **PA che intendono aderire all'Accordo Quadro** possono approfondire le modalità di adesione consultando le informazioni incluse nell'area pubblica del Portale e, se interessate, possono accedere ad un'area informativa ad hoc contenente la documentazione ufficiale – normativa, tecnologica e operativa – per l'AQ nonché una guida alla stima utile a valutare la previsione di spesa generata dall'attivazione di un Contratto Esecutivo. Le **PA che hanno aderito e sono accreditate**, insieme ai rispettivi Fornitori, possono accedere al Portale per

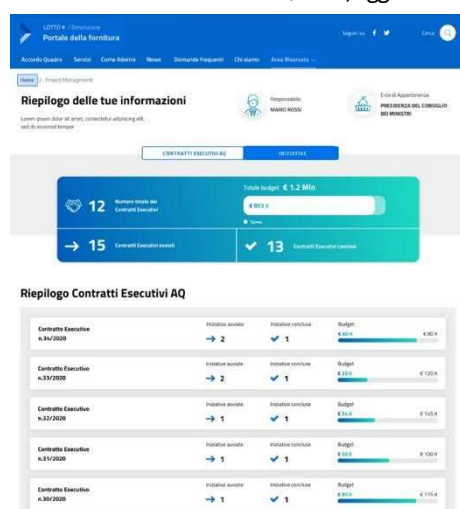




alimentare le informazioni sui servizi attivati, possono usufruire di strumenti di gestione e monitoraggio delle iniziative attivate nonché accedere alle soluzioni di collaborazione individuate per favorire la comunicazione e lo scambio di informazioni, opinioni ed esperienze con le altre PA. Gli **Stakeholder Istituzionali** (Consip ed Agid) possono effettuare verifiche di competenza e monitorare l'andamento delle progettualità e quindi dell'AQ tramite reportistica avanzata.

<b>Accesso (esemplificativo):</b>		<b>Pubblico</b>					<b>Riservato</b>	
AREA		Utente non autenticato	Utente accreditato	Amministrazione che intende aderire all'AQ	Amministrazione che ha aderito all'AQ	Organismi di Coordinamento e Controllo	Stakeholder istituzionali (Consip e AgID)	
Comunicazione		●	●	●	●	●	●	
Informativa			●	●	●	●	●	
Project Management					●	●	●	
Collaborazione e Monitoraggio					●	●	●	
Osservatorio						●	●	

Il portale è organizzato secondo le seguenti aree, la cui rappresentazione esemplificativa in tabella prevede profili e politiche di accesso che saranno da concordare con Consip e AgID in fase di attivazione: ● **AREA COMUNICAZIONE** (funzionalità ad accesso pubblico): L'Area **Comunicazione** è accessibile a tutti gli utenti. Tramite l'Home Page del Portale (Area Comunicazione) vengono messi a disposizione contenuti quali: news inerenti alle Pubbliche Amministrazioni, l'iter di adesione all'Accordo Quadro, aggiornamenti sulle evoluzioni della PA per i cittadini e le imprese. Le Pubbliche Amministrazioni che vogliono valutare la



possibilità di adesione all'Accordo Quadro possono consultare gli "step" previsti per l'accreditamento e cercare le risposte alle domande più frequenti, piuttosto che comunicare il proprio interesse ad avviare un Contratto Esecutivo. La dimostrazione di interesse avviene secondo un processo strutturato che permette di identificare univocamente la Pubblica Amministrazione che fa richiesta ● **AREA INFORMATIVA** : Area nella quale sarà possibile: → esaminare documenti inerenti i servizi previsti dall'Accordo Quadro (con descrizione puntuale degli stessi – **catalogo servizi**) e i modelli operativi previsti dalla fornitura; → consultare i **modelli (prototipi) di Progetto di Sicurezza** (§4.1.1); → confrontarsi con una guida alla stima per visualizzare la previsione di spesa legata ai servizi dell'Accordo Quadro. ● **AREA PROJECT MANAGEMENT**: L'Area **Project Management** è dedicata alla gestione dei singoli Contratti Esecutivi. È organizzata in modo da fornire alle Amministrazioni una visione di insieme sullo stato delle attività e la possibilità di governare ciascun servizio attivato. Nell'Area di Project Management è possibile gestire il workflow dei deliverable di fornitura, consultandone quindi il relativo stato di approvazione. ● **AREA COLLABORAZIONE E MONITORAGGIO**: L'Area **Collaborazione e Monitoraggio** permette agli Stakeholder Istituzionali, a Consip e agli Organismi di Coordinamento e Controllo (OCC), in virtù del ruolo specifico, di

disporre di un quadro univoco sull'Accordo Quadro e sull'andamento delle attività. La rappresentazione individuata è **immediata e intuitiva**, con uno stile di comunicazione efficace. L'Area è organizzata in macro-tematiche di riferimento che permettono un approfondimento per categoria di report. Ogni categoria di report esposta potrà essere esplosa per fornire un monitoraggio di dettaglio sull'avanzamento delle varie progettualità e per avviare un'analisi sugli **indicatori di digitalizzazione: indicatori generali**, suddivisi a loro volta in **indicatori quantitativi**, volti a misurare dati quantitativi come riduzione di tempi e spesa, **indicatori qualitativi**, che permettono di misurare il livello di qualità della Fornitura in modo da identificare eventuali azioni contrattuali da intraprendere, ed **indicatori di collaborazione e riuso**, dedicati invece alla misurazione degli elementi di riuso; un **indicatore di progresso** dell'intervento ottenuto attraverso la realizzazione dell'Ordinativo di Fornitura, volto a calcolare il grado di mappatura di ciascuna classe di **controlli ABSC** (Agid Basic Security Control). **Per le singole PA aderenti all'Accordo Quadro il monitoraggio sarà relativo ai soli servizi attivati e relativo all'andamento degli stessi.** ● **AREA OSSERVATORIO**: L'Area Osservatorio è finalizzata alla presentazione di una **reportistica dedicata ai dati relativi alla qualità e alla sicurezza sui servizi erogati presenti in AQ**, consentendo agli OCC e a Consip di svolgere le proprie funzioni di monitoraggio. Tutti i report saranno prodotti mensilmente in modo automatico ed estraibili a richiesta.

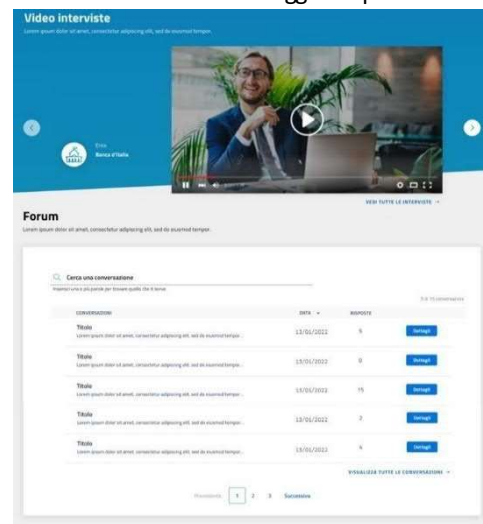
**10.2 STRUMENTI DI ANALISI DEI DATI E REPORTING** Nell'area riservata del Portale è possibile consultare, all'interno di un cruscotto centralizzato, i dati relativi all'Accordo Quadro e ai Contratti Esecutivi in termini di economics, iniziative e servizi avviati e andamento dei servizi stessi. Tali funzionalità potranno beneficiare altresì degli input provenienti dagli ecosistemi di Innovazione proposti dal RTI (§14). La landing page dell'Area Monitoraggio prevede un'area che consente di supervisionare l'intero Accordo Quadro **raccordando tutte le iniziative avviate a partite dai dati elementari** che sono raccolti e rappresentati sia a livello aggregato sia per singolo servizio. La progettazione della reportistica prevede, per ciascun ambito della Fornitura (servizio o progetto), che i dati possano essere utilizzati a diversi livelli di aggregazione, con dettagli differenti e visualizzabili tramite le rappresentazioni grafiche ritenute più opportune ed efficaci per una corretta fruizione. Per ogni report, infatti, se il patrimonio informativo lo permette, è possibile effettuare un **drill-down** sui dati accedendo a tutti i dettagli e dati raccolti per il calcolo dell'indicatore. Il monitoraggio delle iniziative e dei progetti si avvale della possibilità di verificarne e seguirne anche la diffusione in termini di territorio, della tipologia di Amministrazione (PAC, PAL, ecc.), e della diffusione territoriale dei progetti su base tecnologica, individuando cluster e strategia d'adozione sempre maggiormente personalizzati. Attraverso la stessa pagina principale legata ai temi di monitoraggio, è possibile inoltre controllare in maniera rapida e intuitiva lo stato d'avanzamento dei singoli progetti verificando le milestone raggiunte da ciascuno e in maniera aggregata, e verificare l'**andamento dei servizi erogati** tramite il monitoraggio degli indicatori di qualità e la **performance dei servizi**. Rilevante è, inoltre, anche l'area dedicata al monitoraggio economico, basato



sulla declinazione in termini di importi (disponibili ed erogati) della spesa dedicata ai singoli progetti: esplodendo la pagina sul dettaglio di un singolo progetto, infatti, se ne visualizza l'importo complessivo, lo spaccato per erogato e disponibile e le previsioni di consumo per le milestone non ancora raggiunte. Accanto ai prospetti dei dati elementari, è inoltre possibile gestire: **indici statistici** (ad es. percentuali di consumo, di impegno, ecc.); **ricezione di notifiche** (nel caso di possibili sforamenti dei massimali contrattuali, dovuti ad un eccesso di impegni derivanti da iniziative in fase di definizione dei fabbisogni); **le stime a finire** secondo diversi scenari sia a livello di fornitura complessiva, sia a livello di singolo servizio al fine di monitorare l'andamento dei servizi. Inoltre, lo strumento consente anche di lavorare con funzionalità di **self-reporting**, rendendo accessibili le funzioni dello strumento di BI per il disegno e la produzione di report in modalità "self service".

**10.3 SOLUZIONI, PROCESSI E STRUMENTI DI COMUNICAZIONE E DI COLLABORAZIONE IN CHIAVE "SOCIAL"** Il Portale della Fornitura dà spazio alla creazione di una **solida rete di comunicazione e collaborazione**: → risulta aperto ad acquisire dati dagli utilizzatori stessi, da altri portali di forniture concomitanti e dagli open data condivisi dalle Pubbliche Amministrazioni sul sito *dati.gov.it*; → integra diversi strumenti di comunicazione, come tool di messaggistica broadcast verso Amministrazioni e newsletter, quali ad esempio la Privacy Highlights (§9.1.1), dedicata alle principali novità legislative e avvenimenti privacy; → favorisce l'interazione tra cittadini, imprese e PA; → garantisce trasparenza, partecipazione e collaborazione. I meccanismi e i processi di comunicazione e collaborazione con le Amministrazioni contraenti saranno effettuati attraverso il Portale, in linea con quanto riportato nella Procedura di Coordinamento Generale e nelle Procedure di Coordinamento specifiche per ogni Contratto Applicativo, come riportato nella Soluzione Organizzativa. **10.3.1 AREA COLLABORAZIONE E MONITORAGGIO** Come strumento di **Collaborazione e Comunicazione**, all'interno della pagina "Area Collaborazione e Monitoraggio" è presente una

sottosezione **Forum** che permette a tutte le PA aderenti di visualizzare e interagire nelle conversazioni più recenti in merito a diverse categorie (quali ad esempio "Attivazione nuova iniziativa", "Gestione anomalie", "Varie"), con **funzione di ricerca ed evidenza della preview della conversazione**, dell'Ente/Nome utente che ha avviato la stessa e del numero di risposte; la sottosezione può scorrere in modo da visualizzare tutte le anteprime così come presentate e in ordine cronologico; cliccando su una delle conversazioni si accede alla relativa pagina nella quale è possibile interagire con altri utenti utilizzando un servizio di messaggistica; cliccando invece su "Forum" si accede ad una pagina dedicata che permette anche l'apertura di un nuovo thread o la gestione dei filtri per una migliore visualizzazione delle discussioni già aperte. Tra gli ulteriori strumenti in chiave "Social" il RTI propone una Piattaforma di **Digital Storytelling**, fruibile sempre nella pagina "Area Collaborazione e Monitoraggio" per consentire alle Amministrazioni che lo desiderano, secondo le proprie specifiche esigenze, di condividere con altre Amministrazioni e/o Stakeholder le Lesson Learned raccontando in un breve video oppure in un webinar le caratteristiche peculiari dei progetti seguiti con il RTI, promuovendo il riuso e le attività di comunicazione e collaborazione. La Piattaforma ha a disposizione un'intuitiva interfaccia grafica che



permette di selezionare le iniziative suddivise anche per tipologia, Ecosistema AgID ed indicatori di Digitalizzazione. **10.3.2 COLLABORAZIONE IN CHIAVE "SOCIAL"** La soluzione proposta per la collaborazione all'interno dei Team di Progetto impegnati sui Contratti Esecutivi, tenendo conto delle possibilità di utilizzo delle PA che hanno aderito all'AQ, è lo strumento **Microsoft Teams**, volto a ottimizzare in tutto e per tutto la produttività. È un prodotto che unifica i diversi canali di comunicazione (E-mail, Team meeting, chat) e permette a tutti gli stakeholders (in locale o da remoto) di collaborare e aumentare la produttività dei diversi deliverables della fornitura in tempo reale e su diversi dispositivi. Gli utenti riescono ad avere tutto a portata di mano: file condivisi tra tutto il team; chat; Apps scelte come Add-In utili per la gestione del progetto (Planner, PMO, Power BI, SharePoint, Flow, etc.); pianificazioni di riunioni; e altre funzioni utili.

#### 11 MIGLIORAMENTO SOGLIE INDICATORI DI QUALITÀ' – RLFN – Rilievi sulla fornitura

Con riferimento a quanto indicato nell'appendice 1 al CTS lotto 2 "Indicatori di qualità", il RTI si impegna a garantire una riduzione dei valori di soglia previsti secondo le indicazioni di seguito riportate: Valore di soglia **RLFN = 1**.

#### 12 MIGLIORAMENTO SOGLIE INDICATORI DI QUALITÀ' – SLSC – Rispetto di una scadenza contrattuale

Con riferimento a quanto indicato nell'Appendice 1 al CTS Lotto 2 "Indicatori di qualità", il RTI si impegna a garantire una riduzione dei valori di soglia previsti secondo le indicazioni di seguito riportate: Valore di soglia **SLSC = 1**.

#### 13 MIGLIORAMENTO SOGLIE INDICATORI DI QUALITÀ' – NAPP – Non approvazione di documenti

Con riferimento a quanto indicato nell'Appendice 1 al CTS Lotto 2 "Indicatori di qualità", il RTI si impegna a garantire una riduzione dei valori di soglia previsti secondo le indicazioni di seguito riportate: Valore di soglia **NAPP = 0**.

#### 14 INNOVAZIONE

Al fine di rispondere adeguatamente alle esigenze di innovazione connesse ai servizi del presente AQ, il RTI metterà a disposizione i seguenti elementi distintivi:

**1. Processo definito e consolidato per la gestione degli elementi di innovazione** in ambito ai servizi richiesti dalle Amministrazioni, rendendo l'innovazione **sistematica** per indirizzare efficacemente le esigenze attuali ed emergenti. **2. Accesso costante ed immediato all'ecosistema** dell'innovazione, fornito dalla **Mandataria** attraverso gli accordi stipulati tra la struttura **Deloitte Officine Innovazione** ed i protagonisti del processo di innovazione quali **Università, Centri di ricerca, Venture capitalist, Startup ed Acceleratori (vedi Allegato 14.A)**. **3. Coinvolgimento in qualità di mandante della PMI Innovativa Teleco** (Aut. MISE 220439), attiva nella ricerca e sviluppo di soluzioni ed approcci innovativi mediante l'utilizzo di tecnologie emergenti (Big Data & Analytics, 3D User Experience, Internet of Things, Smart & Intelligent Building). **4. Il RTI potrà inoltre coinvolgere nell'ambito di una collaborazione continuativa la Fondazione Bruno Kessler**, prestigioso **Ente di Ricerca** specializzato in cybersecurity, per lo sviluppo di metodologie ed approcci a fronte di evoluzioni normative, cambiamenti di scenario tecnologico ed evoluzione del sistema di cybersecurity.

**14.1 SOGGETTI COINVOLTI E LORO PRINCIPALI CARATTERISTICHE.** Il RTI articolerà i contributi innovativi previsti in ambito ai servizi richiesti, avvalendosi di una serie di presidi, risorse e competenze che costituiranno l'**Ecosistema Interno** (es: Centri di Competenza) e l'**Ecosistema Esterno** (es: Osservatori e Centri di

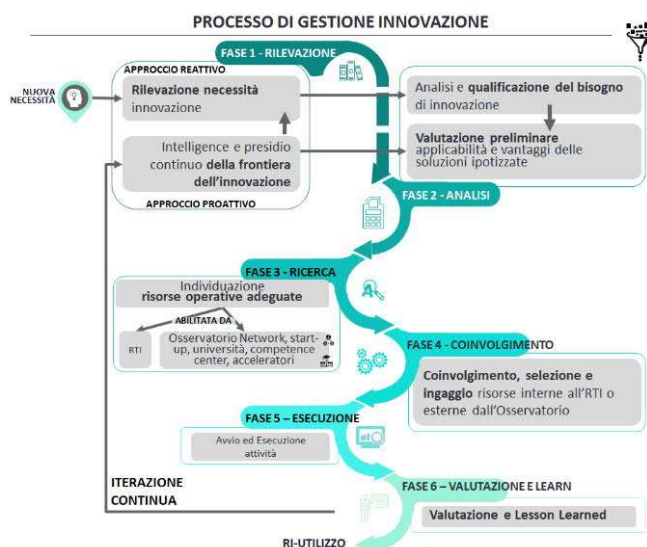
Ricerca) di Innovazione che rappresentano nel complesso l'**Innovation Hub** descritto in precedenza (§ 3.1.1), funzionali a garantire: 1)**Innovazione dei processi/servizi**, attraverso ●attività di **Ricerca e Sviluppo** promosse ed eseguite dalle unità operative dedicate all'innovazione di **DRA ed EYA** e delle capacità della **PMI Innovativa Teleco Srl**, nonché della **Fondazione Bruno Kessler**, Ente di Ricerca specializzato in cybersecurity che il RTI potrà coinvolgere nell'ambito di una collaborazione continuativa ●**Centri di competenza** come **Deloitte Officine Innovazione** che promuove la cultura dell'innovazione e fornirà al RTI ed alle Amministrazioni nuovi servizi per lo sviluppo e il consolidamento delle iniziative di innovazione, con focus sulle tecnologie utili per la trasformazione del business (RPA, AI, canali digitali, Cloud) e la sua protezione ●**Centri di eccellenza di OT/IoT Security** specializzati nell'attività di analisi, sviluppo e test di sicurezza.

2)**Innovazione dei prodotti/tecnologie e relativi acceleratori**, come l'**EY Funding4Innovation** o **Deloitte Switch2Product** (in collaborazione il **PoliHub – Politecnico di Milano**) che definisce strategie di Innovazione in linea con le opportunità di finanziamento per innovazione, trasformazione digitale, Health 4.0 (PNRR, Horizon 2020, PON e POR, fondi europei, nazionali e regionali) e guida startup e scale-up nell'accesso ai finanziamenti e nello sviluppo di soluzioni prototipali da integrare nel business aziendale.

3)**un servizio dinamico di Osservatorio di startup, acceleratori e competenze** in ambito cybersecurity abilitato da numerose iniziative come B Heroes (programma per l'innovazione rivolto in particolare alla promozione di giovani imprese), Premio EY Startup dell'anno (riconoscimento di EY al fine di dare spazio e visibilità a personalità giovani e brillanti che sono riusciti a dar vita ad un'impresa), Premio Marzotto (competizione che premia un'idea imprenditoriale in grado di generare un impatto economico - sociale positivo), Open Italy Startup Accelerator (contest che ha l'obiettivo di favorire la collaborazione tra grandi imprese, Startup italiane/PMI e abilitatori d'innovazione), al fine di fornire, sulla base di cambiamenti ed evoluzioni del mercato, le migliori soluzioni cyber in termini di innovazione.

#### 14.2 AMBITO DI INTERVENTO E VALORE AGGIUNTO APPORTATO.

Di seguito si riporta una proposta preliminare di ambiti di intervento e valore aggiunto concreto, in termini di **innovazione e qualità**, apportato ai servizi richiesti, che rappresenta alcune delle peculiarità e competenze dei soggetti individuati e che possono evolvere ulteriormente sulla base delle esigenze che emergeranno durante l'intera durata del contratto.



Soggetto primario coinvolto	Ambito di intervento ipotizzato	Valore aggiunto
<b>L2.S16 – SECURITY STRATEGY</b>		
Deloitte Officine Innovazione / EY Funding4Innovation	Identificazione di soluzioni e tecnologie emergenti ed innovative sviluppate da startup e PMI innovative, a livello nazionale e internazionale, attraverso l'ecosistema di osservatori permanenti e all'iniziativa di sostegno di ricerca e sviluppo in seno ai soggetti del RTI	Disponibilità di informazioni tempestive ed accurate di tecnologie/soluzioni emergenti che consentono all'Amministrazione di essere aggiornata rispetto alle evoluzioni ed ai trend di mercato
<b>L2.S16 – SECURITY STRATEGY / L2.S17 – VULNERABILITY ASSESSMENT</b>		
Teleco/FBK	Adozione di soluzioni e tecnologie innovative in ambito big-data e intelligenza artificiale, per supportare la creazione di un repository nazionale delle principali vulnerabilità individuate nelle Amministrazioni, alimentato dalle attività completate nel servizio VA ed opportunamente anonimizzate, per fornire una vista centralizzata di analisi e trend statistici aggregati (e.g. top vulnerability, incidenza per dimensioni/sotto ambiti, remediation più comuni), utili anche come input ulteriore alle attività di security strategy. Analogo approccio è proposto per elaborare ed analizzare i dati di benchmark di cui dispone il RTI (§4.4)	Disponibilità di analisi e trend di settore e tipologia di Amministrazione, in termini di <b>esposizione al rischio reale</b> , basata sull'aggregazione di dati utili (risultati VA e benchmark) a ● focalizzare gli interventi prioritari nei PdS ● fornire input di valore ai servizi di prevenzione e gestione delle minacce oggetto del Lotto 1 ● focalizzare l'esecuzione di specifici servizi (PT) su ambiti/tecnologie più vulnerabili ● ottenere una vista aggregata dei principali trend ed analisi di settore
<b>L2.S17 – VULNERABILITY ASSESSMENT / L2.S22 – PENETRATION TESTING</b>		
Teleco/FBK	Disponibilità di soluzioni per la rilevazione automatizzata, basata su tecnologie di intelligenza artificiale (es. le reti neurali di tipo convoluzionale), di anomalie e vulnerabilità su ambienti Cloud e dispositivi IoT (ideale per analisi effettuate su dispositivi con limitate capacità di calcolo, inclusi sistemi di videosorveglianza, sonde e sensoristica, access point wireless, ecc.). Ad esempio, due strumenti automatici open-source sono particolarmente rilevanti: <b>TLS Assistant</b> (inserito nel catalogo del software open source a disposizione della PA, fornito dal Dipartimento per la Trasformazione Digitale e AgID, in grado di analizzare le implementazioni del protocollo TLS alla base di HTTPS e scopre le relative vulnerabilità) e <b>MQTT Security Assistant</b> (in grado di individuare vulnerabilità in ambienti basati su MQTT, uno dei protocolli di riferimento in ambito IoT)	Qualità, efficacia e completezza dei risultati in termini di identificazione delle vulnerabilità su ambienti Cloud ed IoT Riduzione dei tempi e costi di esecuzione associati alle attività di VA e PT
<b>L2.S23 – COMPLIANCE NORMATIVA</b>		



Deloitte/EY/ Teleco/FBK	<b>Osservatorio Privacy</b> finalizzato a recepire ed analizzare tempestivamente l'evoluzione normativa relativamente ai temi Privacy, Provvedimenti del Garante Privacy, opinion del EDPB, ecc. che possono avere impatto sull'Amministrazione. Tale rilevazione è garantita dall'utilizzo di <b>soluzioni basate su tecnologie di intelligenza artificiale ed analisi semantica</b> per acquisire e notificare automaticamente notizie, pubblicazioni, ecc. in ambito Privacy	Qualità, tempestività, completezza e pertinenza delle progettualità e degli interventi legati alla conformità normativa, garantire del continuo aggiornamento del settore
----------------------------	---	---

**14.3 MODALITÀ ORGANIZZATIVE DEL COINVOLGIMENTO.** Per garantire un **elevato livello di innovazione nell'erogazione dei servizi di gara**, il RTI propone un processo di **Gestione dell'Innovazione** che valorizzi tutti gli elementi distintivi e di unicità del RTI stesso, in termini di **modalità organizzative** utili a facilitare la collaborazione di tutte le risorse previste nella soluzione organizzativa, sia con ottica di **efficiente gestione interna che interazione esterna verso le Amministrazioni**, strutturato su un approccio ciclico (continuous monitoring). Si riportano di seguito le fasi che compongono il processo di gestione dell'innovazione.

● **Fase 1:** Rilevazione dell'esigenza sulla base di un duplice approccio. **Reattivo:** a fronte di una richiesta ricevuta. **Proattivo:** attraverso attività di monitoraggio e presidio continuo della frontiera dell'innovazione.

● **Fase 2:** Analisi dell'esigenza di innovazione e valutazione dell'applicabilità delle soluzioni ipotizzate.

● **Fase 3:** Individuazione delle risorse operative adeguate.

● **Fase 4:** Coinvolgimento delle risorse individuate.

● **Fase 5:** Avvio ed Esecuzione attività.

● **Fase 6:** Valutazione e Lesson Learned. Per meglio rappresentare le modalità organizzative del coinvolgimento delle strutture e degli operatori selezionati, il RTI propone una modalità di risposta attraverso l'**Ecosistema Interno**, volto ad indirizzare le esigenze attraverso l'utilizzo di soluzioni innovative interne al RTI, e l'**Ecosistema Esterno**, funzionale a intercettare soluzioni attraverso l'osservazione di trend, soluzioni e strumenti innovativi di mercato.

**Ecosistema interno:** a valle della rilevazione dell'esigenza, le strutture interne al RTI saranno tempestivamente attivate dal RUAC CE o dal Referente Tecnico CE, per il tramite dell'**Innovation Leader** (§ 3.1.1.), secondo il seguente approccio: 1) **ricerca delle competenze** interne al RTI necessarie a soddisfare l'esigenza espressa dall'Amministrazione, ottimizzando le tempistiche di avvio delle attività; 2) **selezione del team**, condivisione/approvazione da parte dell'Amministrazione; 3) **integrazione delle competenze** individuate nel team e avvio attività.

**Ecosistema esterno:** sulla base di un'analisi proattiva degli Osservatori o nel caso in cui sia opportuna una sinergia tra le competenze/soluzioni interne al RTI e di mercato, eventuali ulteriori Startup e PMI innovative saranno ingaggiate secondo il seguente approccio: 1) **preselezione di un cluster** che include tipicamente fino a 10 operatori (in funzione dell'aderenza delle soluzioni proposte rispetto all'esigenza di innovazione ed al contesto dell'Amministrazione, ad esempio operatori con caratteristiche di prossimità geografica e attinenza alla tematica innovativa di interesse); 2) **valutazione e selezione di un massimo di 2-3 operatori** (short list) per la definizione di prototipi e/o lo sviluppo di soluzioni-pilota.



Ciascun operatore sarà valutato, in particolare, in funzione di appositi criteri (es. innovatività della soluzione offerta, funzionalità e servizi offerti, radicamento sul territorio, referenze PA ed extra PA, valore economico), opportunamente prioritizzati in coerenza con il contesto dell'Amministrazione coinvolta; 3) **selezione** della struttura/operatore più idonea. Successivamente sarà effettuata l'attivazione della struttura/operatore selezionato secondo modalità e tempi concordati di concerto con l'Amministrazione. Le **tempistiche di ingaggio dell'ecosistema interno**, essendo basate sui soggetti già parte del RTI (vedi PMI

Innovativa) e/o vincolate da accordi di collaborazione già stipulati (ad esempio Ente di ricerca), seguono le **tempistiche di evasione** dei servizi. Il completamento delle fasi 1-3 dell'**ecosistema esterno**, avviandosi già nella fase di definizione dei fabbisogni, rispetterà le tempistiche di ingaggio previste per ciascun servizio.

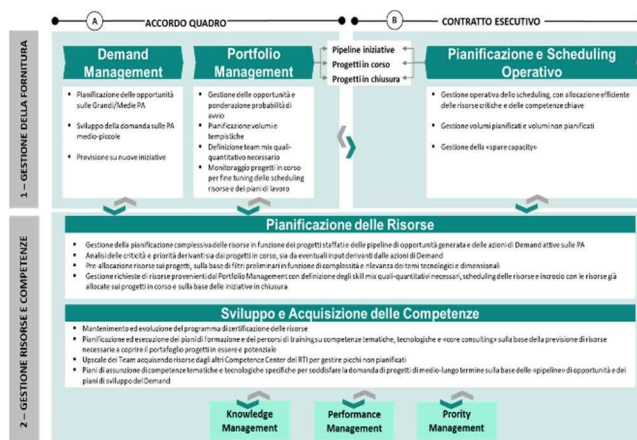
## 15 FLESSIBILITÀ DELLE RISORSE

La variabilità delle esigenze, dei requisiti e dei possibili contesti tecnologici e gestionali rappresenta una peculiarità dell'ambito della Pubblica Amministrazione ben nota alle aziende del RTI, che **erogano da diverso tempo servizi in modalità simile** e per le quali tale complessità rappresenta una modalità di lavoro **"business as usual"**. In questo ambito, il **modello organizzativo ed operativo** adottato dal RTI per la gestione flessibile di risorse si basa su:

- la **comprovata esperienza** maturata dalle aziende del RTI: ogni anno sono gestiti in media più di 2000 progetti con caratteristiche comparabili con i programmi previsti dal CTS, anche in termini di estemporaneità nell'attivazione e variabilità dei requisiti;
- la **capacità previsionale** sui tempi d'attivazione dei progetti, basata sui progetti suddetti già condotti, che consente di mobilitare le risorse con tempi medi inferiori ai 15 giorni;
- la possibilità di far leva su un considerevole **bacino di risorse interne distribuito geograficamente** che è costituito per i temi di Cyber Security da più di 500 risorse in Italia e 3000 in EMEA. Queste sono supportate sul territorio nazionale da **3 Centri di Competenza** (Milano, Roma e Bari), **1 Centro di Delivery** (Bari), **2 Cyber Intelligence Center** (Milano e Roma) e da una rete di più di 500 consulenti tra fornitori accreditati e professionisti altamente qualificati ed accuratamente selezionati.

La gestione della flessibilità operativa del RTI si basa sull'interazione tra (vedi figura): A) processi operativi di gestione dell'Accordo Quadro e B) processi di attuazione dei progetti dei Contratti Esecutivi (CE); e tra 1) gestione della Fornitura nel suo complesso e 2) gestione delle risorse e delle competenze all'interno delle aziende. Le caratteristiche del modello organizzativo sono:

- **Gestione proattiva della Demand.** L'approccio del RTI è primariamente proattivo e mira a implementare un processo di gestione della Demand robusto, che riduca le esigenze di gestione e mitigazione dei rischi a

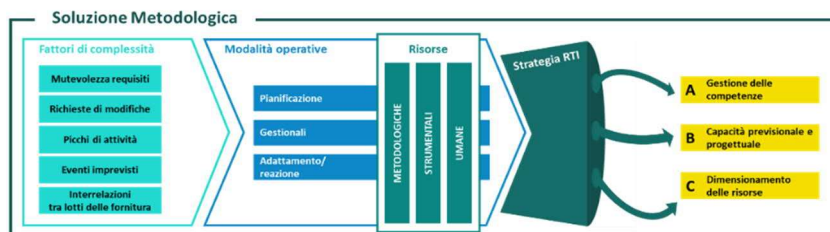




posteriori e limiti la numerosità di risposte reattive alle esigenze e ai problemi imprevisi. ● **Gestione del Portfolio Management.** L'azione strutturata del PMO AQ, di concerto con i RUAC CE, nonché il recepimento di richieste provenienti dalle Amministrazioni, consentono di definire le opportunità, identificando volumi e tempistiche di avvio ed incanalandole efficientemente nell'ambito della pipeline complessiva in ottica di Portfolio Management. ● **Pianificazione operativa.** I RUAC CE, in collaborazione con il Resource Manager, individuano le professionalità più adeguate per soddisfare le richieste della singola Amministrazione e pianificano le risorse sul singolo CE. ● **Pianificazione delle Risorse.** Il Resource Manager ottimizza la pianificazione delle risorse tenendo in considerazione sia i progetti in corso che quelli in chiusura, sia le priorità che le indicazioni provenienti dalla Demand. ● **Sviluppo e Acquisizione delle Competenze.** Il Knowledge Manager lavora costantemente nell'analisi del portafoglio iniziative per definire i piani di sviluppo e crescita delle risorse, inoltre supporta il Resource Manager nel confrontare la pipeline ponderata dei progetti in ingresso con i volumi di risorse disponibili. ● Il modello operativo di gestione delle risorse, inoltre, si avvale anche dei processi standard di **knowledge management**, di **performance management** per allocare le competenze "giuste" al posto "giusto" e **priority management** per gestire eccezioni e "scalare" in caso di problemi.

**15.1 DISPONIBILITÀ E TEMPESTIVITÀ DI ALLOCAZIONE DELLE RISORSE PROFESSIONALI** L'approccio per garantire - in modo **strutturato** e **proattivo** - la **disponibilità e tempestività delle risorse** tiene conto di una serie di fattori di complessità quali: la **necessità di erogare nuovi progetti, più progetti in contemporanea verso la stessa Amministrazione o più Amministrazioni** dislocate diversamente a livello geografico, **variabilità dei requisiti, richieste di modifiche** pianificate o estemporanee, **picchi di attività** ed **eventi imprevisi**. A tale complessità, il RTI risponde con: ● **Modalità operative di pianificazione** volte a realizzare tutte quelle azioni interne al RTI che **riducono il rischio di progetti estemporanei e picchi di attività**; ● **Modalità operative gestionali**, che includono le **azioni atte a gestire le possibili variazioni del contesto**, in termini di nuovi progetti, variazione dei requisiti dei progetti esistenti, esigenze non pianificate e contrazione dei tempi che impattano sugli interventi in corso e che richiedono una revisione della pianificazione delle attività e delle risorse; ● **Modalità operative di adattamento e reazione**, ossia azioni forti e veloci di contenimento e ripristino dei livelli standard di erogazione dei servizi che limitano gli impatti sulla normale esecuzione delle attività. Tali modalità operative sono abilitate dall'utilizzo di specifiche risorse **metodologiche**, orientate alla gestione dei rischi, da risorse **strumentali**, che supportano i processi di pianificazione, e da risorse **umane**, selezionate dal bacino a disposizione del RTI, per garantire al RTI l'apporto di adeguato know-how e di background di esperienze. Il RTI propone quindi una specifica **strategia di flessibilità nella gestione delle risorse** incentrata sui seguenti elementi:

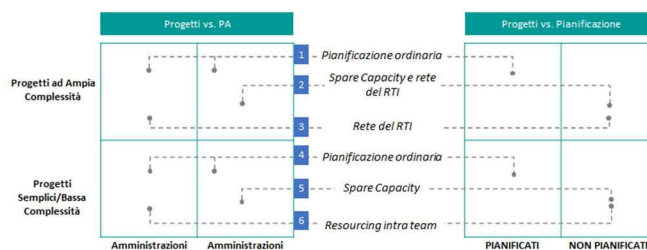
A) **Gestione delle competenze:** per garantire la disponibilità delle risorse, il RTI adotta un processo centralizzato di selezione delle risorse affidata al **Resource Manager** che si avvale di una **Mappa delle Competenze**, costantemente aggiornata, per individuare risorse con skill adeguate e conoscenza del contesto. La disponibilità di un quadro di insieme di tutte le competenze



richieste dalla Fornitura e la **ridondanza delle skill sul gruppo di lavoro**, ottenuta grazie alle azioni di formazione, abilita la possibilità di disporre di **risorse qualificate ed attivarle tempestivamente** sulla base delle specifiche richieste delle Amministrazioni. Per garantire la flessibilità nella gestione e nell'inserimento delle risorse, il RTI propone un modello operativo T-Shaped. Tale approccio interdisciplinare è applicato all'interno di tutti i servizi e comprende lo sviluppo di:

→ **competenze verticali:** la singola risorsa è specializzata in un ambito di riferimento; → **competenze orizzontali:** la stessa risorsa approfondisce progressivamente anche altre tematiche affini al proprio ambito di riferimento, fungendo da possibile risorsa aggiuntiva in caso di picco che richieda le stesse competenze. B) **Capacità previsionale e progettuale:** comprende tutte le azioni realizzabili al fine di: ● **Prevenire l'avvio delle nuove progettualità** grazie sia alla capacità del RTI di monitorare l'evoluzione del contesto di business, normativo e tecnologico, sia all'analisi costante del flusso di progetti già attivati nell'ambito dell'AQ. ● **Stimare l'effort e le competenze necessarie per gestire la domanda** sulla base delle esperienze progettuali già svolte ed individuare, già in fase di pianificazione, ogni elemento che potrebbe generare un effort diverso da quanto previsto. C) **Dimensionamento delle risorse:** la disponibilità delle risorse sui progetti è garantita da un processo strutturato di dimensionamento che prevede: ● l'identificazione, sulla base delle esigenze rilevate, delle figure professionali da impiegare sui singoli CE con le relative competenze; ● l'analisi del bacino di disponibilità delle risorse da cui verranno selezionate quelle che comporranno i Team di lavoro; ● l'aggiornamento del bacino di disponibilità in funzione degli interventi attivati; ● il dimensionamento/ridimensionamento del Team. L'accurato processo di gestione delle competenze, capacità previsionali ed una solida metodologia di dimensionamento delle risorse in funzione delle attività consente di **efficientare l'impiego** delle risorse e garantirne la **tempestività nell'allocazione** sulle singole progettualità.

**15.2 METODOLOGIE E STRUMENTI PROPOSTI PER LA FLESSIBILITÀ NELLA GESTIONE DI PIÙ CONTRATTI IN CONTEMPORANEA.** Metodologie per la gestione di più contratti in contemporanea - Il modello operativo proposto per gestire più contratti in contemporanea si basa sulla dimensione di complessità delle Amministrazioni, definita mediante il modello di classificazione già presentato per la definizione dei PdS (§4.1.1.1), e sulle diverse tipologie dimensionali/complessità dei progetti che saranno affrontati dal RTI. In questo contesto, l'approccio metodologico consiste in: 1) Classificazione delle esigenze progettuali e modalità di gestione (vedi figura): ● **i progetti di tipo "1" e "4"** sono accuratamente e preventivamente pianificati, anche grazie alle strutture di presidio del RTI, e rientrano nell'ordinaria gestione e pianificazione delle risorse del Resource Manager ● **i progetti di tipo "2"** hanno generalmente una probabilità bassa di accadimento. In questi casi, i progetti saranno organizzati in logica di **"spare capacity"** ossia mediante **capacità disponibile nel bacino** a disposizione del RTI e, qualora non sufficiente, tramite la rete di fornitori e professionisti esterni al RTI ● **i progetti di tipo "3"** rappresentano situazioni imprevedibili che, per il modello di presidio posto in essere dal RTI, non dovrebbero manifestarsi. Qualora questo tipo di progetti dovessero comunque presentarsi, saranno gestiti attingendo alla rete di esterni del RTI; ● **i progetti di tipo "5"** sono gestiti in logica di **"spare capacity"** in modalità **"first in – first out"** in modo da **acquisire e smaltire**



**piccole iniziative “on demand”** senza impattare sulle pianificazioni dei grandi progetti • **i progetti di tipo “6”**, essendo comunque riferiti ad Amministrazioni presidiate, sono gestiti attingendo alle risorse disponibili all'interno dei team di presidio (resourcing intra team). 2) **Gestione di una molteplicità di progetti in contemporanea**. L'eventuale insorgenza di **molteplici progetti** generati dalle Amministrazioni è gestita dal RTI in maniera proattiva mediante il PMO AQ che, supportato dal Resource Manager, seleziona le azioni necessarie alla gestione di più progetti in contemporanea tramite la **ridefinizione delle priorità ed il ricorso a tecniche di resource sharing**, in particolare: • **resource sharing intra aree di competenza tematico/funzionale** della stessa Fornitura: consente una rapida integrazione di risorse tenuto conto del basso gap formativo; • **resource sharing intra team RTI** consente lo spostamento temporaneo di risorse da altri servizi con competenze analoghe e con minimo effort di allineamento sui progetti; • **riorganizzazione dei team di lavoro** con integrazione di risorse da altre aree di competenza del RTI sulla Fornitura che richiede un periodo di allineamento e formazione rispetto alla specifica necessità; • **ricorso a CdC e CdD**: in caso di necessità ci si potrà avvalere del **supporto dei Centri di Competenza e del Centro di Delivery**, sfruttando modalità di “rapid learning” per il riallineamento sui contenuti mancanti in modalità veloce e puntuale, rispetto alla specifica competenza richiesta; • **coinvolgimento di risorse** dalla rete del RTI costituita da fornitori accreditati e professionisti specializzati, per integrare eventuali skill specifici sul progetto.

**Strumenti.** Per la gestione integrata dei progetti e delle risorse, il RTI si avvarrà di un set integrato di strumenti correntemente utilizzati per pianificare le risorse sui progetti e gestire la formazione e le performance. Questi strumenti sono rispettivamente aggiornati e mantenuti da funzioni aziendali dedicate alle tematiche di Learning e Planning: • **La Mappa delle Competenze (SKILL)** del personale del RTI è gestita con **MyCompetencies** uno strumento che censisce il catalogo delle conoscenze necessarie (tematico / normative e tecnologiche) distinte per figura professionale e fornisce una vista di tutte le potenziali risorse allocabili sulla Fornitura con le competenze richieste, e tramite **PeopleNetwork**, un sistema globale e cross-function, che contiene tutti i dettagli sui profili e sulle competenze delle risorse e che si integra con il sistema di pianificazione StaffIt; • **StaffIt** offre la possibilità di gestire e programmare la disponibilità operativa delle risorse, assegnando la persona giusta al progetto giusto in termini di aree geografiche e per le diverse linee di business; • **MERA** è lo strumento dedicato allo **Scheduling Operativo**. Utilizzato da tutto il personale, permette di verificare, in ogni momento, il timing dell'impiego di ciascuna risorsa in uno specifico progetto e gli impegni futuri. L'incrocio tra pianificazione “actual” e fabbisogni complessivi derivati dal modulo **MERA** fornisce indicazione su dimensionamento preliminare del gap di risorse da coprire e tempistiche entro le quali deve essere coperto in funzione delle date avvio stimate dei progetti.







## 16 AGGIORNAMENTO DELLE RISORSE PROFESSIONALI

Il modello organizzativo ed operativo per l'aggiornamento delle risorse professionali è incentrato sullo **sviluppo di piano di formazione e relativi contenuti**, che si integra con l'evoluzione del contesto normativo e tecnologico e le necessità delle Amministrazioni. Si propone dunque un processo di **formazione continua basata sui fabbisogni per l'erogazione dei servizi**, al fine di supervisionare lo svolgimento dei percorsi di aggiornamento delle competenze necessarie e l'eventuale introduzione di nuove risorse professionali.

**16.1 SOLUZIONI PROGETTUALI E STRUMENTI PER GARANTIRE LA FORMAZIONE E L'AGGIORNAMENTO CONTINUO - Soluzione progettuale.** Al fine di garantire la **formazione e l'aggiornamento continuo, tematico e tecnologico** delle risorse del RTI, si applicherà il **modello formativo ben consolidato nell'ambito del RTI costituito da un processo ciclico/continuativo in più fasi**, così articolato: 1) redazione del **piano delle competenze necessarie** per l'erogazione dei servizi. Tale strumento viene costantemente aggiornato durante l'intera Fornitura per **rilevare in modo continuativo nuove esigenze** e fabbisogni formativi soddisfatti dagli interventi effettuati. L'utilizzo della mappa delle competenze, inoltre, consente una più facile **individuazione delle risorse adeguate a svolgere i servizi**, garantendo non solo la costituzione di team in linea con le esigenze e gli obiettivi dell'Amministrazione rispetto ad una particolare attività, ma anche l'integrazione degli stessi, ove necessario, con risorse specializzate dei Centri di Competenza; 2) analisi e **censimento delle competenze** presenti nell'ambito del RTI e di quelle da acquisire nella prospettiva di evoluzioni previste nell'ambito dei servizi della Fornitura. L'assessment è svolto con il supporto di griglie di valutazione delle competenze a duplice compilazione: una sezione compilata dalle risorse stesse per censire le proprie esperienze e competenze; una seconda sezione compilata dai Responsabili dei Team con le valutazioni sulla qualità dei progetti realizzati, le esigenze delle Amministrazioni, le evoluzioni normative, tecnologiche ed organizzative in corso; 3) **identificazione dei gap** esistenti tra il **fabbisogno di competenze** emerso durante la prima fase e le **competenze presenti** nei Team evidenziate nella seconda fase. L'obiettivo di questa analisi è proiettare sull'asse temporale della Fornitura il divario tra le competenze delle risorse professionali a disposizione e quelle che saranno nel tempo necessarie, prevedibili a partire dalle esigenze rilevate dal Demand Management, nonché dalle evoluzioni organizzative, normative e tecnologiche attese. L'**analisi** di questi **scostamenti** consentirà di **indirizzare il piano formativo** verso obiettivi chiari e circoscritti; 4) **predisposizione del piano di formazione**: individuazione e definizione degli interventi formativi e del dettaglio **delle singole iniziative** (modalità di erogazione, contenuti, risorse target, calendario, strumenti a supporto, ecc.); 5) **erogazione degli interventi formativi**: questa fase prevede la realizzazione di corsi di formazione sia in **modalità tradizionali** (formazione d'aula e *training on-the-job*) sia tramite strumenti più innovativi basati su una **didattica applicativa/esperienziale** (*business case, role playing*). La metodologia didattica sarà individuata in relazione alla tipologia di risorse coinvolte e al servizio sul quale sono impiegate. I vantaggi a cui si tende sono: a) maggiore personalizzazione della proposta educativa; b) processi di apprendimento diversificati e autonomi; c) aumento del livello di interesse e della motivazione delle risorse coinvolte; 6) **valutazione degli interventi**: sono previsti momenti strutturati di valutazione dei corsi, fra i quali: a) questionari di valutazione delle competenze acquisite da ogni risorsa, da svolgere al termine dei moduli/percorsi formativi, disegnato e proposto in modalità elettronica; b) questionari compilati dal responsabile della risorsa partecipante, dopo qualche settimana di impegno nelle attività contrattuali, come riscontro delle capacità dimostrate. In particolare, saranno adottati **knowledge enablers**, quali **risorse senior (nel ruolo di counselor)**, dei **Centri di Competenza** e di **collaborazioni col personale docente del mondo accademico**. Le aziende del RTI hanno, inoltre, costituito dei percorsi formativi dedicati ai professionisti targettizzati per tutti i livelli, basati sul modello della transformative leadership e sul modello delle competenze del futuro elaborato dalle aziende. Si basano su più pilastri volti a rafforzare le competenze che sostengono le **trasformazioni di processo, tecnologiche e digitali**: • **Formazione Trasversale**: è mirata al raggiungimento della Personal Excellence e della Engagement Excellence con corsi su

competenze critiche con il fine ultimo di raggiungere il successo nell'era trasformativa. ● **Formazione Tecnica:** il percorso è verticale e specifico per competenze, allineato alla struttura organizzativa della consulenza di business e tecnologica, prevedendo quindi learning path altamente specialistici. ● **Programmi formativi mirati:** programmi di formazione mirati allo sviluppo di conoscenze, esperienze e competenze indispensabili per comprendere a fondo scenari e dinamiche del mondo business e technology da utilizzare nell'ambito dei servizi. **Strumenti tecnologici** - Il RTI dispone di **portali e strumenti dedicati alla formazione e all'aggiornamento continuo delle risorse**. Di seguito i principali:

LEARNING	 <b>Success Factor:</b> è il portale attraverso il quale le risorse EY possono gestire la propria carriera e il percorso di crescita e selezionare corsi di formazione inerenti il proprio percorso. Nello specifico, il portale consente alle risorse di gestire la propria formazione accedendo al "Learning Roadmap" e il proprio percorso formativo, contenente i corsi obbligatori e quelli selezionati nell'ambito della definizione degli obiettivi definiti per ogni risorsa. Il portale offre la possibilità di predisporre iniziative personalizzate che mirano al consolidamento e potenziamento di skill e conoscenze possedute dalla risorsa supportandola nel proprio percorso di crescita sulla base delle proprie esigenze e quelle della Fornitura.
	 <b>Saba Cloud:</b> è la piattaforma di gestione della formazione in Deloitte, mediante la quale è possibile iscriversi ai corsi in presenza o in virtual classroom, monitorare i corsi in scadenza, accedere ai corsi di formazione obbligatoria in base al ruolo, grado e business di appartenenza, generare report e certificati dei corsi completati.
COMPETENZE	 <b>EY My Competencies:</b> è il tool di mappatura delle competenze che consente di tracciare le esperienze maturate e le <i>skill</i> delle risorse. Sulla base di specifici bisogni individuati, è possibile identificare in tempi rapidi le risorse più idonee da coinvolgere nei Team, garantendo un processo snello per l'attivazione dei professionisti presso l'Amministrazione.
	 <b>Deloitte People Network:</b> è lo strumento di Deloitte che contiene tutti i profili delle risorse, indicandone, tra le altre, background e competenze maturate, costituendo una sorta di combinazione tra una people directory e un social network che consente l'individuazione tempestiva delle risorse e delle relative competenze.

**16.2 PROPOSTA DI PIANO FORMATIVO.** L'approccio identificato garantisce la formazione e l'aggiornamento continuo delle risorse del RTI, che viene declinato nel piano formativo. Le esigenze formative sono individuate da un lato in base al tipo di servizio da erogare e le relative competenze e conoscenze che questo richiede, e dall'altro tenendo in considerazione l'evoluzione del contesto in cui sono erogati i servizi che consente una completezza di copertura delle tematiche anche nel corso del tempo. In particolare, potranno essere pianificati interventi ad hoc per rispondere a necessità formative che si dovessero manifestare nel corso dell'erogazione dei servizi derivanti da cambiamenti del contesto quali: ● **evoluzioni normative** che impattano sulla Pubblica Amministrazione e sui servizi erogati, per i quali il RTI è in grado di anticiparne l'effetto sfruttando gli osservatori normativi a propria disposizione e prevedendo iniziative di addestramento delle risorse coinvolgendo anche gli esperti della propria rete; ● **evoluzioni degli scenari** di attacco cibernetici e delle vulnerabilità dei sistemi, per i quali si prevede il costante aggiornamento delle risorse maggiormente dedicate all'erogazione dei servizi di verifica tecnica della sicurezza tramite periodiche sessioni di allineamento con i centri di competenza dei network delle aziende del RTI, esercitazioni e simulazioni in laboratorio nonché partecipazione a seminari dedicati; ● **evoluzioni delle tecnologie** in uso presso le Amministrazioni e degli strumenti di sicurezza adottati, per i quali il RTI prevede la formazione delle risorse mediante corsi ad hoc e workshop con i principali vendor, anche tramite le partnership in essere. Il RTI intende, inoltre, progettare e attuare, per la presente Fornitura, una serie di **azioni finalizzate ad incrementare le competenze delle risorse e a renderle immediatamente operative** nello svolgimento delle attività. Nell'ambito del piano operativo saranno pertanto adottati i seguenti strumenti: ● welcome kit, con brochure e documenti di base inerenti le informazioni principali sul contesto della Fornitura, ovvero una raccolta selezionata di materiale informativo che fornisce una panoramica sulle tematiche di interesse, consentendo a ogni nuova risorsa un rapido ed efficace orientamento in modalità self training ● percorso di addestramento personalizzato sulla base delle competenze in possesso della nuova risorsa e delle specifiche competenze richieste in funzione del ruolo che questa andrà a ricoprire ● tutoring, con cui le risorse più esperte saranno coinvolte per svolgere attività di affiancamento e addestramento delle risorse negli aspetti funzionali e tecnici di erogazione del servizio e l'uso degli strumenti di conoscenza disponibili ● percorsi di certificazione mirati che consentono il mantenimento e l'aggiornamento delle certificazioni professionali già in possesso delle risorse nonché il conseguimento di nuove certificazioni che si renderanno necessarie in base all'evoluzione del contesto: il RTI garantisce in particolare che le nuove release delle certificazioni previste e le scadenze dei certificati già conseguiti saranno gestiti proattivamente in modo tale da: → consentire il conseguimento di nuove certificazioni in breve tempo dalla pubblicazione dei corsi relativi a nuove release; → consentire alle risorse le cui certificazioni sono in scadenza di conseguire una nuova certificazione che estende il periodo di validità senza soluzione di continuità ● interventi formativi dedicati: mediante realizzazione di corsi di formazione sia in modalità tradizionali che tramite strumenti più innovativi basati su una didattica applicativa/esperienziale, funzionali all'erogazione dei servizi ● accesso alla knowledge base di Fornitura rigorosamente alimentata e aggiornata, e ricorso frequente a tecniche di knowledge sharing, attraverso la diffusione di informazioni, conoscenze e best practice, che permettono un facile e rapido allineamento delle persone coinvolte nei team, anche in caso di sostituzione o integrazione delle risorse. Al termine di ogni attività di formazione, è aggiornata la Mappa delle Competenze utilizzata per la gestione e l'allocazione delle risorse sulle progettualità.

## 17 ASSUNZIONE DELLE RISORSE PROFESSIONALI

Con riferimento al complesso delle assunzioni necessarie per ogni contratto esecutivo finanziato, in tutto o in parte, con le risorse previste dal Regolamento (UE) 2021/240 del Parlamento europeo e del Consiglio del 10 febbraio 2021 e dal Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021, nonché dal PNC, e fermo restando il rispetto del requisito necessario di cui al CTS Generale al par. 7.1, il RTI si impegna ad assumere persone disabili, giovani di qualsiasi genere, con età inferiore a trentasei anni, e donne per l'esecuzione di ciascun contratto esecutivo o per la realizzazione di attività ad essi connessi o strumentali, nella misura di seguito riportata: **>35,01%**.

**ALLEGATO B – OFFERTA ECONOMICA DEL FORNITORE**

<b>Offerta economica relativa a:</b>	
Numero Gara	2860180
Nome Gara	Gara a procedura aperta per la conclusione di un Accordo Quadro ai sensi del D.Lgs. 50/2016 e s.m.i., suddivisa in due lotti, avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni – ID 2296
Criterio di Aggiudicazione	Gara ad offerta economicamente più vantaggiosa
Lotto	1 (Servizi di compliance e controllo)

<b>AMMINISTRAZIONE TITOLARE DEL PROCEDIMENTO</b>	
Amministrazione	CONSIP SPA
Partita IVA	05359681003
Indirizzo	VIA ISONZO 19/E - ROMA (RM)

<b>CONCORRENTE</b>	
Forma di Partecipazione	R.T.I. costituendo (D.Lgs. 50/2016, art. 48, comma 8)
Ragione Sociale	DELOITTE RISK ADVISORY S.R.L. (mandataria) Società a Responsabilità Limitata
Partita IVA	05059250158
Codice Fiscale Impresa	05059250158
Provincia sede registro imprese	MI
Numero iscrizione registro imprese	05059250158
Codice Ditta INAIL	13540154/98
n. P.A.T.	(DIRIGENTI)-020025790 (SUPPORT)-090946121 (REVISORI) 092149724
Matricola aziendale INPS	4964035450 03
CCNL applicato	COMMERCIO TERZIARIO, DIRIGENTI COMMERCIO, DIRIGENTI INDUSTRIA
Settore	TERZIARIO



Indirizzo sede legale	VIA TORTONA, 25 - MILANO (MI)
Telefono	06478051
Fax	0283341161
PEC Registro Imprese	DRA@DELOITTE.LEGALMAIL.IT
Ragione Sociale	EY ADVISORY S.P.A. (mandante) Società per Azioni
Partita IVA	13221390159
Codice Fiscale Impresa	13221390159
Provincia sede registro imprese	MI
Numero iscrizione registro imprese	1627915
Codice Ditta INAIL	13244823
n. P.A.T.	90447620/40
Matricola aziendale INPS	4962267996
CCNL applicato	COMMERCIO
Settore	CONSULENZA AZIENDALE
Indirizzo sede legale	VIA MERAVIGLI N.14 - MILANO (MI)
Telefono	06675351
Fax	06675351
PEC Registro Imprese	EYADVISORY@LEGALMAIL.IT
Ragione Sociale	TELECO S.R.L. (mandante) Società a Responsabilità Limitata
Partita IVA	02856220922
Codice Fiscale Impresa	02856220922
Provincia sede registro imprese	RM
Numero iscrizione registro imprese	02856220922
Codice Ditta INAIL	14009171
n. P.A.T.	20269280/16
Matricola aziendale INPS	1706999698
CCNL applicato	TELECOMUNICAZIONI
Settore	INDUSTRIA
Indirizzo sede legale	VIA ROSAZZA 26 - ROMA (RM)
Telefono	0705435000
Fax	0702330631
PEC Registro Imprese	TELECO@PEC.IT
<b>Offerta sottoscritta da</b>	<b>TROGU FIORENZO, FERSURELLA LORENZO, BERGAMO DARIO</b>

Scheda di Offerta	
Descrizione	Servizi di compliance e controllo - offerta economica
Offerta Economica	
Parametro Richiesto	Valore Offerto
1 - L1.S16 - Security Strategy - gg/p Team ottimale - Prezzo unitario offerto (€)	250
2 - L1.S17 - Vulnerability Assessment - gg/p Team ottimale - Prezzo unitario offerto (€)	165
3 - L1.S18 -Testing del codice - Statica - Singola esecuzione - Prezzo unitario offerto (€)	1309
4 - L1.S18 -Testing del codice - Statica - Fascia 1 - Fino a 15 applicazioni - Prezzo unitario offerto (€)	1100
5 - L1.S18 -Testing del codice - Statica - Fascia 2 - Fino a 50 applicazioni - Prezzo unitario offerto (€)	1047
6 - L1.S18 -Testing del codice - Statica - Fascia 3 - > 50 applicazioni - Prezzo unitario offerto (€)	982
7 - L1.S19 - Testing del codice - Dinamica - Gold - Fascia 1 - Fino a 15 applicazioni - Prezzo unitario offerto (€)	2067
8 - - Gold - Fascia 2 - Fino a 50 applicazioni - Prezzo unitario offerto (€)	1571
9 - - Gold - Fascia 3 - > 50 applicazioni - Prezzo unitario offerto (€)	1179
10 - - Silver - Fascia 1 - Fino a 15 applicazioni - Prezzo unitario offerto (€)	1113
11 - - Silver - Fascia 2 - Fino a 50 applicazioni - Prezzo unitario offerto (€)	916
12 - - Silver - Fascia 3 - > 50 applicazioni - Prezzo unitario offerto (€)	827
13 - - Bronze - Fascia 1 - Fino a 15 applicazioni - Prezzo unitario offerto (€)	482

14 - - Bronze - Fascia 2 - Fino a 50 applicazioni - Prezzo unitario offerto (€)	414
15 - - Bronze - Fascia 3- > 50 applicazioni - Prezzo unitario offerto (€)	345
16 - L1.S20 -Testing del codice - Mobile - Fascia 1 - Fino a 15 applicazioni - Prezzo unitario offerto (€)	1600
17 - L1.S20 -Testing del codice - Mobile - Fascia 2 - Fino a 50 applicazioni - Prezzo unitario offerto (€)	1450
18 - L1.S20 -Testing del codice - Mobile - Fascia 3 - > 50 applicazioni - Prezzo unitario offerto (€)	1398
19 - L1.S21 -Supporto all'analisi e gestione degli incidenti - gg/p Team ottimale - Prezzo unitario offerto (€)	170
20 - L1.S22 -Penetration testing - gg/p Team ottimale - Prezzo unitario offerto (€)	165
21 - L1.S23 -Compliance normativa - gg/p Team ottimale - Prezzo unitario offerto (€)	170
Ribasso medio ponderato - Calcolato dal Sistema	0,58608

**Il Concorrente, nell'accettare tutte le condizioni specificate nella documentazione del procedimento, altresì dichiara:**

- che la presente offerta è irrevocabile ed impegnativa sino al termine di conclusione del procedimento, così come previsto nella lex specialis;
- che la presente offerta non vincolerà in alcun modo la Stazione Appaltante/Ente Committente;
- di aver preso visione ed incondizionata accettazione delle clausole e condizioni riportate nel Capitolato Tecnico e nella documentazione di Gara, nonché di quanto contenuto nel Capitolato d'oneri/Disciplinare di gara e, comunque, di aver preso cognizione di tutte le circostanze generali e speciali che possono interessare l'esecuzione di tutte le prestazioni oggetto del Contratto e che di tali circostanze ha tenuto conto nella determinazione dei prezzi richiesti e offerti, ritenuti remunerativi;
- di non eccepire, durante l'esecuzione del Contratto, la mancata conoscenza di condizioni o la sopravvenienza di elementi non valutati o non considerati, salvo che tali elementi si configurino come cause di forza maggiore contemplate dal codice civile e non escluse da altre norme di legge e/o dalla documentazione di gara;
- che i prezzi/sconti offerti sono onnicomprensivi di quanto previsto negli atti di gara;
- che i termini stabiliti nel Contratto e/o nel Capitolato Tecnico relativi ai tempi di esecuzione delle prestazioni sono da considerarsi a tutti gli effetti termini essenziali ai sensi e per gli effetti dell'articolo 1457 cod. civ.;
- che il Capitolato Tecnico, così come gli altri atti di gara, ivi compreso quanto stabilito relativamente alle modalità di esecuzione contrattuali, costituiranno parte integrante e sostanziale del contratto che verrà stipulato con la stazione appaltante/ente committente.

**ATTENZIONE: QUESTO DOCUMENTO NON HA VALORE SE PRIVO DELLA  
SOTTOSCRIZIONE A MEZZO FIRMA DIGITALE**

**ALLEGATO C – CORRISPETTIVI E TARIFFE PAL**



**ACCORDO QUADRO PER L’AFFIDAMENTO SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI AI SENSI DELL’ART. ex art. 54, co. 4 lett. a) DEL d.lgs. N. 50/2016 – ID 2296**

**Lotto 2 - Servizi di compliance e controllo per le Pubbliche Amministrazioni Locali (PAL)**

Servizio	Id.	Voce economica	Prezzo offerto
L1.S16 - Security Strategy	1	gg/p Team ottimale	€ 250,00
L1.S17 - Vulnerability Assessment	2	gg/p Team ottimale	€ 165,00
L1.S18 - Testing del codice - Statica	3	Singola esecuzione	€ 1.309,00
	4	Fascia 1 - Fino a 15 applicazioni	€ 1.100,00
	5	Fascia 2 - Fino a 50 applicazioni	€ 1047,00
	6	Fascia 3 - > 50 applicazioni	€ 982,00
L1.S19 - Testing del codice - Dinamica	7	Gold - Fascia 1 - Fino a 15 applicazioni	€ 2.067,00
	8	Gold - Fascia 2 - Fino a 50 applicazioni	€ 1.571,00
	9	Gold - Fascia 3 - > 50 applicazioni	€ 1.179,00
	10	Silver - Fascia 1 - Fino a 15 applicazioni	€ 1.113,00
	11	Silver - Fascia 2 - Fino a 50 applicazioni	€ 916,00
	12	Silver - Fascia 3 - > 50 applicazioni	€ 827,00
	13	Bronze - Fascia 1 - Fino a 15 applicazioni	€ 482,00
	14	Bronze - Fascia 2 - Fino a 50 applicazioni	€ 414,00
	15	Bronze - Fascia 3- > 50 applicazioni	€ 345,00
L1.S20 - Testing del codice - Mobile	16	Fascia 1 - Fino a 15 applicazioni	€ 1.600,00
	17	Fascia 2 - Fino a 50 applicazioni	€ 1.450,00
	18	Fascia 3 - > 50 applicazioni	€ 1.398,00
L1.S21 -Supporto all’analisi e gestione degli incidenti	19	gg/p Team ottimale	€ 170,00

L1.S22 -Penetration testing	20	gg/p Team ottimale	€ 165,00
L1.S23 -Compliance normativa	21	gg/p Team ottimale	€ 170,00

## **ALLEGATO D – PATTO D'INTEGRITA'**

**CLASSIFICAZIONE DEL DOCUMENTO: CONSIP PUBLIC**

**PATTO DI INTEGRITA' RELATIVO ALLA PROCEDURA DI GARA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI – ID 2296**

**LOTTO 2**

**ALLEGATO D**

**PATTO DI INTEGRITA' AI SENSI DELLA L. 190/2012**

Classificazione del documento: Consip Public

Accordo Quadro con più operatori economici ai sensi dell'art. 54, comma 4, lettera a) del D.Lgs. 50/2016, per la fornitura di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni – ID SIGEF 2296

Lotto 2

Allegato D – Patti di integrità

## SOMMARIO

1. OGGETTO .....	2
2. AMBITO DI APPLICAZIONE .....	2
3. OBBLIGHI DEL FORNITORE .....	3
4. OBBLIGHI DI CONSIP .....	Errore. Il segnalibro non è definito.
5. SANZIONI .....	4
6. AUTORITÀ COMPETENTE IN CASO DI CONTROVERSIE.....	6

Classificazione del documento: Consip Public

Accordo Quadro con più operatori economici ai sensi dell'art. 54, comma 4, lettera a) del D.Lgs. 50/2016, per la fornitura di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni – ID SIGEF 2296

Lotto 2

Allegato D – Patti di integrità



## PREMESSA

L'art. 1, comma 17 della L. 6 novembre 2012, n. 190 (*"Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione"*) dispone che *"le stazioni appaltanti possono prevedere negli avvisi, bandi di gara o lettere di invito che il mancato rispetto delle clausole contenute nei protocolli di legalità o nei patti di integrità costituisce causa di esclusione dalla gara"*.

Il Piano Nazionale Anticorruzione, approvato con delibera n. 72/2013 dall'Autorità Nazionale Anticorruzione e successivamente aggiornato, prevede che le pubbliche amministrazioni e le stazioni appaltanti, in attuazione del citato art. 1, comma 17 della L. 190/2012, predispongono e utilizzano protocolli di legalità o patti di integrità per l'affidamento di appalti pubblici. A tal fine, i predetti soggetti inseriscono negli avvisi, nei bandi di gara e nelle lettere di invito la clausola di salvaguardia che il mancato rispetto del protocollo di legalità o del patto di integrità dà luogo all'esclusione dalla gara e alla risoluzione del contratto.

L'ANAC, inoltre, con il parere 11/2014, si è espressa favorevolmente riguardo alla previsione del bando che richiede l'accettazione dei protocolli di legalità e dei patti di integrità quale possibile causa di esclusione, *"in quanto tali mezzi sono posti a tutela di interessi di rango sovraordinato e gli obblighi in tal modo assunti discendono dall'applicazione di norme imperative di ordine pubblico, con particolare riguardo alla legislazione in materia di prevenzione e contrasto della criminalità organizzata nel settore degli appalti"*.

Infine il presente patto recepisce le raccomandazioni fornite dall'ANAC con le Linee Guida n. 15 del 12 luglio 2019.

In attuazione di quanto sopra,

## SI CONVIENE QUANTO SEGUE

### ART. 1 OGGETTO

1. Il presente patto di integrità (di seguito, il **"Patto di Integrità"**) stabilisce la reciproca e formale obbligazione

– tra

- la Consip S.p.A. a socio unico in qualità di stazione appaltante (di seguito, anche **"Consip"**),
- i soggetti legittimati, sulla base della normativa vigente, ad utilizzare l'Accordo Quadro (di seguito, anche le **"Amministrazioni"** o la **"singola Amministrazione contraente"**)
- l'operatore economico partecipante alla procedura di gara (di seguito anche il **"Concorrente"**);
- l'aggiudicatario della procedura di gara (di seguito, anche il **"Fornitore"**) relativa alla stipula dell'Accordo Quadro ovvero dei Contratti esecutivi a valere sull'Accordo Quadro per l'affidamento dei servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni".

a conformare i propri comportamenti ai principi di lealtà, trasparenza e correttezza, impegnandosi ciascuno, per quanto di rispettiva competenza, a contrastare fenomeni di corruzione e illegalità e comunque a non compiere alcun atto volto a distorcere o influenzare indebitamente il corretto svolgimento di tutte le fasi dell'appalto, dalla partecipazione alla procedura alla esecuzione dell'Accordo Quadro e dei singoli Contratti esecutivi successivamente affidati.

2. Il Fornitore, la Consip e le Amministrazioni si impegnano a rispettare nonché a far rispettare al rispettivo personale, ai collaboratori e, per quanto riguarda il Fornitore, anche ai subappaltatori/subcontraenti/imprese ausiliarie, il presente Patto di Integrità, il cui spirito e contenuto condividono pienamente, informando gli stessi prontamente e puntualmente e vigilando scrupolosamente sulla loro osservanza.

### ART. 2 AMBITO DI APPLICAZIONE

1. Il presente Patto di Integrità regola i comportamenti di tutti i soggetti individuati nel precedente art. 1, ed è vincolante:

Classificazione del documento: Consip Public

Accordo Quadro con più operatori economici ai sensi dell'art. 54, comma 4, lettera a) del D.Lgs. 50/2016, per la fornitura di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni – ID SIGEF 2296

Lotto 2

Allegato D – Patti di integrità

- **per Consip S.p.A.** nella fase di espletamento della procedura di gara dell'Accordo Quadro
- **per le Amministrazioni:** nella fase di esecuzione dell'Accordo Quadro nonché nella fase di esecuzione degli Contratti esecutivi;
- **per l'Operatore Economico,** nella fase di svolgimento della procedura di gara per la stipula di Accordi Quadro e dei relativi Contratti esecutivi.
- **per il Fornitore,** nella fase di esecuzione dell'Accordo Quadro e dei Contratti esecutivi.

2. Il Patto di Integrità costituisce parte integrante e sostanziale dell'Accordo Quadro e dei singoli Contratti esecutivi successivamente affidati.

### **ART. 3 OBBLIGHI DEL CONCORRENTE E DEL FORNITORE**

#### **1. Obblighi del Concorrente:**

- a1) il Concorrente s'impegna a non corrispondere né promettere di corrispondere ad alcuno – direttamente o tramite terzi, ivi compresi i soggetti collegati o controllati - somme di denaro o altra utilità ai fini dell'aggiudicazione della gara o di distorcere il corretto svolgimento della stessa;
- b1) il Concorrente dichiara di astenersi dal compiere qualsiasi tentativo di turbativa, irregolarità o, comunque, violazione delle regole della concorrenza ovvero a segnalare tempestivamente a Consip e alla Pubblica Autorità qualsiasi tentativo di turbativa, irregolarità e violazioni delle regole di concorrenza di cui dovesse venire a conoscenza durante tutte le fasi della procedura, fornendo elementi dimostrabili a sostegno delle suddette segnalazioni;
- c1) il Concorrente si impegna a segnalare eventuali situazioni di conflitti di interesse, di cui sia o venga a conoscenza al momento della partecipazione e durante l'espletamento dell'intera procedura rispetto ai soggetti (sia di Consip che delle Amministrazioni) di cui al par. 4 delle Linee Guida Anac sopra richiamate, che siano coinvolti in una qualsiasi fase della procedura (programmazione, progettazione, preparazione documenti di gara, selezione dei concorrenti, aggiudicazione) o che possano influenzarne in qualsiasi modo l'esito in ragione del ruolo ricoperto all'interno dell'ente;
- d1) il Concorrente si impegna a far rilasciare all'impresa ausiliaria, ai fini della partecipazione alla procedura di gara, una dichiarazione di presa visione e accettazione delle clausole del presente Patto di integrità;
- e1) il Concorrente si impegna ad inserire nei contratti di avvalimento una clausola che prevede l'impegno dell'ausiliaria a rispettare gli obblighi di cui al Patto di integrità, pena la risoluzione del contratto di avvalimento e il conseguente obbligo per il Concorrente medesimo di sostituire l'impresa ausiliaria nel caso di violazione degli impegni assunti nel medesimo Patto di integrità;
- f1) il Concorrente dichiara di essere a conoscenza del D.Lgs. n. 231/2001 e della L. n. 190/2012 e di aver preso visione della parte generale del Modello di organizzazione, gestione e controllo, del Codice Etico, nonché del Piano triennale per la prevenzione della corruzione e della trasparenza, predisposti da Consip e pubblicati sul sito internet della Società, e di uniformarsi ai principi ivi contenuti che devono ritenersi applicabili anche nei rapporti tra il Fornitore e la Consip S.p.A.;

#### **2. Obblighi del Fornitore:**

- a2) Il Fornitore si impegna a segnalare eventuali situazioni di conflitti di interesse, anche riferite alla fase di partecipazione alla procedura di gara, di cui sia o venga a conoscenza durante l'intera fase esecutiva del Contratto rispetto ai soggetti (sia di Consip che delle Amministrazioni) di cui al par. 4 delle Linee Guida Anac sopra richiamate, che siano coinvolti in una qualsiasi fase della procedura (sottoscrizione del contratto, esecuzione, collaudo, pagamenti) o che possano influenzarne in qualsiasi modo l'esito in ragione del ruolo ricoperto all'interno dell'ente;

Classificazione del documento: Consip Public

Accordo Quadro con più operatori economici ai sensi dell'art. 54, comma 4, lettera a) del D.Lgs. 50/2016, per la fornitura di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni – ID SIGEF 2296

Lotto 2

Allegato D – Patti di integrità

- b2) il Fornitore dichiara di non avere influenzato il procedimento amministrativo diretto a stabilire il contenuto del bando o di altro atto equipollente al fine di condizionare le modalità di scelta del contraente e di non aver corrisposto né promesso di corrispondere ad alcuno direttamente o tramite terzi, ivi compresi i soggetti collegati o controllati - somme di denaro o altra utilità al fine di agevolare o distorcere la corretta e regolare esecuzione dell'Accordo Quadro e dei singoli Contratti esecutivi successivamente affidati;
  - c2) Il Fornitore dichiara di non aver concluso con altri operatori economici alcun tipo di accordo volto ad alterare o limitare la concorrenza, ovvero a determinare un unico centro decisionale ai fini della partecipazione alla procedura di gara e della formulazione dell'offerta, risultata poi essere la migliore.
  - d2) Il Fornitore dichiara di astenersi dal compiere qualsiasi tentativo di turbativa, irregolarità o, comunque, violazione delle regole della concorrenza ovvero a segnalare tempestivamente a Consip, alla Pubblica Autorità e alla singola Amministrazione contraente, qualsiasi tentativo di turbativa, irregolarità e violazioni delle regole di concorrenza di cui dovesse venire a conoscenza durante la fase di esecuzione dell'Accordo Quadro e dei singoli Contratti esecutivi successivamente affidati, fornendo elementi dimostrabili a sostegno delle suddette segnalazioni;
  - e2) il Fornitore si impegna a segnalare a Consip e alla singola Amministrazione contraente, nonché alla Pubblica Autorità competente e alla Prefettura, qualunque tentativo di concussione e qualsiasi illecita richiesta o pretesa da parte dei dipendenti di Consip e/-della singola Amministrazione contraente o di chiunque possa influenzare le decisioni relative all'esecuzione dell'Accordo Quadro e dei singoli Contratti esecutivi successivamente stipulati;
  - f2) il Fornitore si impegna ad inserire nei contratti di subappalto e negli altri subcontratti una clausola che preveda il rispetto degli obblighi di cui al presente Patto di Integrità da parte dei subappaltatori/subcontraenti, e la risoluzione, ai sensi dell'art. 1456 c.c., del contratto di subappalto, nel caso di violazione di tali obblighi da parte di questi ultimi, con conseguente comunicazione a Consip dell'avvenuta risoluzione del predetto contratto;
  - g2) il Fornitore si impegna a rendere noti, su richiesta dell'Amministrazione contraente, tutti i pagamenti eseguiti e riguardanti i Contratti di Fornitura e i singoli Appalti Specifici affidati;
  - h2) il Fornitore dichiara di essere a conoscenza del D.Lgs. n. 231/2001 e della L. n. 190/2012 e di aver preso visione della parte generale del Modello di organizzazione, gestione e controllo, del Codice Etico, nonché del Piano triennale per la prevenzione della corruzione e della trasparenza, predisposti da Consip e pubblicati sul sito internet della Società, e di uniformarsi ai principi ivi contenuti che devono ritenersi applicabili anche nei rapporti tra il Fornitore e la Consip S.p.A. in relazione degli obblighi assunti dal Fornitore nei confronti di quest'ultima.
3. Il Concorrente e il Fornitore dichiarano, inoltre, di essersi già impegnati nei confronti di Consip al rispetto degli obblighi di cui al presente patto di integrità, mediante apposita dichiarazione resa in sede di partecipazione alla procedura di gara.
4. Il Concorrente e il Fornitore prendono atto ed accettano che la violazione, comunque accertata da Consip e/o dalle Amministrazioni di uno o più impegni assunti con il presente Patto di Integrità può comportare l'applicazione delle sanzioni di cui al successivo art. 5.

#### **ART. 4 OBBLIGHI DI CONSIP E DELLE AMMINISTRAZIONI.**

1. Nel rispetto del presente Patto di Integrità, Consip e le Amministrazioni si impegnano, per quanto di rispettiva competenza, a rispettare i principi di lealtà, trasparenza e correttezza di cui alla L. n. 190/2012, nonché, nel caso in cui venga riscontrata una violazione di detti principi o di prescrizioni analoghe, a valutare l'eventuale attivazione di procedimenti disciplinari nei confronti del rispettivo personale a vario titolo intervenuto nella procedura di affidamento e nell'esecuzione dell'Accordo Quadro e dei singoli Contratti esecutivi

Classificazione del documento: Consip Public

Accordo Quadro con più operatori economici ai sensi dell'art. 54, comma 4, lettera a) del D.Lgs. 50/2016, per la fornitura di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni – ID SIGEF 2296

Lotto 2

Allegato D – Patti di integrità

successivamente affidati , secondo quanto previsto dai rispettivi piani di prevenzione della corruzione.

## **ART. 5 SANZIONI**

1. Il Concorrente e il Fornitore prendono atto ed accettano che la violazione degli obblighi assunti con il presente Patto di Integrità, nonché la non veridicità delle dichiarazioni rese, comunque accertati da Consip e/o dalle Amministrazioni, può comportare l'applicazione di una o più delle seguenti sanzioni:
  - a. se la violazione è accertata nella fase precedente all'aggiudicazione dell'Accordo Quadro, esclusione dalla procedura di affidamento anche ai sensi dell'art. 80, comma 5, lettera c-bis del D.lgs. 50/2016, ed eventuale escussione della garanzia provvisoria prestata in favore della Consip, nei casi e nei modi previsti dalla lex specialis di gara;
  - b. se la violazione è accertata nella fase successiva all'aggiudicazione ma precedentemente alla stipula dell'Accordo quadro, revoca dell'aggiudicazione ed escussione della garanzia provvisoria;
  - c. se la violazione è accertata nella fase di esecuzione:

risoluzione ex art. 1456 c.c. dell'Accordo Quadro, nonché incameramento della garanzia definitiva e risarcimento dell'eventuale danno ulteriore, nel caso in cui la violazione degli impegni di cui al precedente art. 3 sia accertata in relazione agli obblighi contrattuali assunti dal Fornitore nei confronti di Consip in forza dell'Accordo Quadro. La risoluzione può essere altresì esercitata ai sensi dell'art. 1456 c.c. i) ogni qualvolta nei confronti del Fornitore, dei suoi dirigenti e/o dei componenti della compagine sociale, sia stata disposta misura cautelare o sia intervenuto rinvio a giudizio per taluno dei delitti di cui agli artt. 317, 318, 319, 319bis, 319ter, 319quater, 320, 322, 322bis, 346bis, 353, 353bis, 355 e 356 c.p. ii) nel caso in cui, violato l'obbligo di segnalazione di cui all'art. 3, lett. e2) che precede, sia stata disposta nei confronti dei "pubblici amministratori"<sup>1</sup> che hanno esercitato funzioni relative alla stipula ed esecuzione del contratto, misura cautelare o sia intervenuto rinvio a giudizio per il delitto previsto dall'art. 317 del c.p.. Nei casi sopra indicati sub i) e ii), Consip eserciterà la potestà risolutoria previa intesa con l'Autorità Nazionale Anticorruzione che potrà valutare se, in alternativa all'ipotesi risolutoria, ricorrano i presupposti per la prosecuzione del rapporto Contrattuale alle condizioni di cui all'art. 32 del D.L. 90/2014 convertito nella legge n. 114/2014. Resta fermo che dell'intervenuta risoluzione dell'Accordo Quadro Consip potrà tenere conto ai fini delle valutazioni di cui all'articolo 80, comma 5, lett. c-ter), del D.Lgs. 50/2016.

La risoluzione dell'Accordo Quadro prevista nel presente Patto di Integrità può costituire condizione risolutiva del singolo Contratto esecutivo;

risoluzione ex art. 1456 c.c. del singolo Contratto esecutivo, nel caso in cui la violazione degli impegni di cui al precedente art. 3 sia accertata in relazione agli obblighi contrattuali assunti dal Fornitore nei confronti della singola Amministrazione contraente nell'ambito del Contratto esecutivo. La risoluzione potrà essere altresì esercitata ai sensi dell'art. 1456 c.c. i) ogni qualvolta nei confronti del Fornitore, dei suoi dirigenti e/o dei componenti della compagine sociale, sia stata disposta misura cautelare o sia intervenuto rinvio a giudizio per taluno dei delitti di cui agli artt. 317, 318, 319, 319bis, 319ter, 319quater, 320, 322, 322bis, 346bis, 353, 353bis, 355 e 356 c.p.; ii) nel caso in cui, violato l'obbligo di segnalazione di cui all'art. 3, lett. e2) che precede, sia stata disposta nei confronti dei "pubblici amministratori" che hanno esercitato funzioni relative alla stipula ed esecuzione del contratto, misura cautelare o sia intervenuto rinvio a giudizio per il delitto previsto dall'art. 317 del c.p.. Nei casi sopra indicati sub i) e ii) l'Amministrazione eserciterà la potestà risolutoria previa intesa con l'Autorità Nazionale Anticorruzione che potrà valutare se, in alternativa all'ipotesi risolutoria, ricorrano i presupposti per la prosecuzione del rapporto contrattuale alle condizioni

---

<sup>1</sup> Per "pubblici amministratori" si intendono i soggetti che hanno esercitato attività di pubblico interesse.

di all'art. 32 del D.L. 90/2014 convertito nella legge n. 114/2014.

La risoluzione del singolo Contratto esecutivo comporterà altresì l'escussione della garanzia definitiva.

In caso di intervenuta risoluzione del Contratto esecutivo su iniziativa della singola Amministrazione contraente, quest'ultima è tenuta a darne tempestiva notizia a Consip, motivandone le ragioni; Consip, a sua volta, ha la facoltà di procedere, ai sensi dell'art. 1456 c.c., alla risoluzione di diritto dell'Accordo Quadro. Resta fermo che dell'intervenuta risoluzione Contratto esecutivo Consip potrà tenere conto ai fini delle valutazioni di cui all'articolo 80, comma 5, lett. c-ter), del D.Lgs. 50/2016;

In ogni caso Consip procederà alla segnalazione del fatto all'ANAC ed alle competenti Autorità giurisdizionali.

#### **ART. 6 AUTORITÀ COMPETENTE IN CASO DI CONTROVERSIE**

Ogni eventuale controversia relativa all'interpretazione e all'esecuzione del presente Patto di Integrità sarà risolta dall'Autorità Giudiziaria competente, secondo quanto nell'Accordo Quadro.

Roma, lì \_\_\_\_ \_\_\_\_

**Il presente Patto di integrità viene allegato quale parte integrante dell'Accordo Quadro.**



**ALLEGATO E – NOMINA E RESPONSABILE DEL TRATTAMENTO DATI**

**CONTRATTO ESECUTIVO NELL'AMBITO DELL'ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I.,  
SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI  
COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI - ID 2296**

**NOMINA RESPONSABILE DEL TRATTAMENTO DEI DATI**

1. Con la sottoscrizione della presente da parte dell'Amministrazione \_\_\_\_\_ il Fornitore \_\_\_\_\_ è nominato Responsabile del trattamento ai sensi dell'art. 28 del Regolamento UE n. 2016/679 sulla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (nel seguito anche "*Regolamento UE*"), per tutta la durata del contratto attuativo (nel seguito anche "*contratto*") relativo alla Convenzione \_\_\_\_\_. A tal fine il Responsabile è autorizzato a trattare i dati personali necessari per l'esecuzione delle attività oggetto del contratto e si impegna ad effettuare, per conto dell'Amministrazione (Titolare del Trattamento), **le sole operazioni di trattamento necessarie per fornire il servizio oggetto del contratto attuativo e della Convenzione**, nei limiti delle finalità ivi specificate, nel rispetto del Regolamento UE 2016/679, del D.Lgs. 196/2003 e s.m.i e del D. Lgs. n. 101/2018 (nel seguito anche "*Normativa in tema di trattamento dei dati personali*"), e delle istruzioni nel seguito fornite.
2. Il Fornitore/Responsabile si impegna a presentare su richiesta dell'Amministrazione garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse per l'adozione di misure tecniche ed organizzative adeguate volte ad assicurare che il trattamento sia conforme alle prescrizioni della normativa in tema di trattamento dei dati personali. Nel caso in cui tali garanzie risultassero insussistenti o inidonee l'Amministrazione potrà chiedere la presentazione di garanzie sufficienti entro un termine congruo ed in caso di mancato riscontro risolvere il contratto con il Responsabile iniziale.
3. Le finalità del trattamento sono: **<Valorizzare in ragione dell'oggetto del contratto \_\_\_\_\_>**
4. Il tipo di dati personali trattati in ragione delle attività oggetto del contratto sono: **<Valorizzare in ragione dell'oggetto del contratto i) dati comuni (es. dati anagrafici e di contatto ecc.); ii) dati sensibili; iii) dati giudiziari>**.
5. Le categorie di interessati sono: **<Valorizzare in ragione dell'oggetto del contratto es. dipendenti e collaboratori, utenti dei servizi, ecc.>**.
6. Nell'esercizio delle proprie funzioni, il Responsabile si impegna a:
  - a) rispettare la normativa vigente in materia di trattamento dei dati personali, ivi comprese le norme che saranno emanate nel corso della durata del contratto;
  - b) trattare i dati personali per le sole finalità specificate e nei limiti dell'esecuzione delle prestazioni contrattuali;
  - c) trattare i dati personali conformemente alle istruzioni impartite dal Titolare e di seguito indicate che il Fornitore si impegna a far osservare anche alle persone da questi autorizzate ad effettuare il trattamento dei dati personali oggetto del presente contratto, d'ora in poi "persone autorizzate"; nel caso in cui ritenga che un'istruzione costituisca una violazione del Regolamento UE sulla protezione dei dati o delle altre disposizioni di legge relative alla protezione dei dati personali, il Fornitore deve informare immediatamente il Titolare del trattamento;
  - d) garantire la riservatezza dei dati personali trattati nell'ambito del presente contratto e verificare che le persone autorizzate a trattare i dati personali in virtù del presente contratto:
    - o si impegnino a rispettare la riservatezza o siano sottoposti ad un obbligo legale appropriato di segretezza;
    - o ricevano la formazione necessaria in materia di protezione dei dati personali;
    - o trattino i dati personali osservando le istruzioni impartite dal Titolare al Responsabile;
  - e) adottare politiche interne e attuare misure che soddisfino i principi della protezione dei dati personali fin dalla progettazione di tali misure (*privacy by design*), nonché adottare misure tecniche ed organizzative adeguate

Classificazione del documento: Consip Public

Accordo Quadro con più operatori economici ai sensi dell'art. 54, comma 4, lettera a) del D.Lgs. 50/2016, per la fornitura di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni – ID SIGEF 2296

Lotto 2

Allegato E – Nomina Responsabile trattamento dati

per garantire che i dati personali siano trattati, in ossequio al principio di necessità ovvero che siano trattati solamente per le finalità previste e per il periodo strettamente necessario al raggiungimento delle stesse (*privacy by default*);

- f) adottare tutte le misure tecniche ed organizzative che soddisfino i requisiti del Regolamento UE anche al fine di assicurare un adeguato livello di sicurezza dei trattamenti, in modo tale da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, modifica, divulgazione non autorizzata, nonché di accesso non autorizzato, anche accidentale o illegale, o di trattamento non consentito o non conforme alle finalità della raccolta;
- g) su eventuale richiesta dell'Amministrazione, assistere quest'ultima nello svolgimento della valutazione d'impatto sulla protezione dei dati personali, conformemente all'articolo 35 del Regolamento UE e nella eventuale consultazione del Garante per la protezione dei dati personali, prevista dall'articolo 36 del medesimo Regolamento UE;
- h) **< tale obbligo non si applica alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato o includa il trattamento di dati sensibili di cui all'articolo 9, paragrafo 1, o i dati giudiziari di cui all'articolo 10, ai sensi dell'art. 30 del Regolamento UE e nei limiti di quanto esso prescrive, tenere un Registro delle attività di trattamento effettuate sotto la propria responsabilità e cooperare con l'Amministrazione e con l'Autorità Garante per la protezione dei dati personali, mettendo il predetto Registro a disposizione del Titolare e dell'Autorità, laddove ne venga fatta richiesta >;**
- i) **< eventuale: adottare le misure minime di sicurezza ICT per le PP.AA. di cui alla Circolare AgID n. 2/2017 del 18 aprile 2017 >.**

7. Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, il Fornitore si impegna a fornire all'Amministrazione un piano di misure di sicurezza rimesso all'approvazione della stessa, che saranno concordate al fine di mettere in atto misure tecniche ed organizzative idonee per garantire un livello di sicurezza adeguato al rischio e per garantire il rispetto degli obblighi di cui all'art. 32 del Regolamento UE. Tali misure comprendono tra le altre, se del caso **< personalizzare in ragione dell'oggetto del contratto >**:

- o la pseudonimizzazione e la cifratura dei dati personali;
- o la capacità di assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi che trattano i dati personali;
- o la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
- o una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

La valutazione circa l'adeguatezza del livello di sicurezza deve tenere conto, in particolare, dei rischi del trattamento derivanti da: distruzione o perdita anche accidentale, modifica, divulgazione non autorizzata, nonché accesso non autorizzato, anche accidentale o illegale, o trattamento non consentito o non conforme alle finalità del trattamento dei dati personali conservati o comunque trattati.

8. Il Responsabile del trattamento deve mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al Regolamento UE, oltre a contribuire e consentire al Titolare - anche tramite soggetti terzi dal medesimo autorizzati, dandogli piena collaborazione - verifiche periodiche circa l'adeguatezza e l'efficacia delle misure di sicurezza adottate ed il pieno e scrupoloso rispetto delle norme in materia di trattamento dei dati personali.

A tal fine, il Titolare informa preventivamente il Responsabile del trattamento con un preavviso minimo di tre **< o diverso termine indicato dalla PA >** giorni lavorativi; nel caso in cui all'esito di tali verifiche periodiche, ispezioni e audit le misure di sicurezza dovessero risultare inadeguate rispetto al rischio del trattamento o, comunque,

Classificazione del documento: Consip Public

Accordo Quadro con più operatori economici ai sensi dell'art. 54, comma 4, lettera a) del D.Lgs. 50/2016, per la fornitura di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni – ID SIGEF 2296

Lotto 2

Allegato E – Nomina Responsabile trattamento dati

inidonee ad assicurare l'applicazione del Regolamento, o risulti che il Fornitore agisca in modo difforme o contrario alle istruzioni fornite dall'Amministrazione, quest'ultima applicherà le penali previste nella Convenzione e diffiderà il Fornitore ad adottare tutte le misure più opportune o a tenere una condotta conforme alle istruzioni entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a seguito della diffida, resa anche ai sensi dell'art. 1454 cc, l'Amministrazione, in ragione della gravità dell'inadempimento, potrà risolvere il contratto ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.

9. **1) (Autorizzazione generale)** Il Responsabile del trattamento può ricorrere ad un altro Responsabile del trattamento (di seguito, "sub-Responsabile del trattamento") per gestire attività di trattamento specifiche, informando, periodicamente \_\_\_\_\_ **(la PA deve specificare la periodicità)**, il Titolare del trattamento delle nomine e delle sostituzioni dei Responsabili. Nella comunicazione andranno specificate le attività di trattamento delegate, i dati identificativi dei sub-Responsabili nominati e i dati del contratto di esternalizzazione. **<Oppure> 2) (Autorizzazione specifica)** Il Responsabile del trattamento può avvalersi di ulteriori Responsabili per delegargli attività specifiche, previa autorizzazione scritta del Titolare del trattamento.
10. Il sub-Responsabile del trattamento deve rispettare obblighi analoghi a quelli forniti dal Titolare al Responsabile Iniziale del trattamento, riportate in uno specifico contratto o atto di nomina. Spetta al Responsabile Iniziale del trattamento assicurare che il sub-Responsabile del trattamento presenti garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per l'adozione di misure tecniche ed organizzative appropriate di modo che il trattamento risponda ai principi e alle esigenze del Regolamento UE. In caso di mancato adempimento da parte del sub-Responsabile del trattamento degli obblighi in materia di protezione dei dati, il Responsabile Iniziale del trattamento è interamente responsabile nei confronti del Titolare del trattamento di tali inadempimenti; l'Amministrazione potrà in qualsiasi momento verificare le garanzie e le misure tecniche ed organizzative del sub-Responsabile, tramite audit e ispezioni anche avvalendosi di soggetti terzi. Nel caso in cui tali garanzie risultassero insussistenti o inidonee l'Amministrazione potrà chiedere la presentazione di garanzie sufficienti entro un termine congruo ed in caso di mancato riscontro risolvere il contratto con il Responsabile iniziale.
- Nel caso in cui all'esito delle verifiche, ispezioni e audit le misure di sicurezza dovessero risultare inapplicate o inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del Regolamento o risulti che il sub responsabile agisca in modo difforme o contrario alle istruzioni fornite dall'Amministrazione, quest'ultima applicherà al Fornitore/Responsabile Iniziale del trattamento le penali previste nella Convenzione e diffiderà lo stesso a far adottare al sub-Responsabile del trattamento tutte le misure più opportune o a tenere una condotta conforme alle istruzioni entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a tale diffida, resa anche ai sensi dell'art. 1454 cc, l'Amministrazione potrà, in ragione della gravità dell'inadempimento, risolvere il contratto attuativo con il Responsabile iniziale ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.
11. Il Responsabile del trattamento deve assistere il Titolare del trattamento al fine di dare seguito alle richieste per l'esercizio dei diritti degli interessati. Qualora gli interessati esercitino tale diritto presso il Responsabile del trattamento, quest'ultimo è tenuto **<selezionare una tra le due opzioni:**
- 1)** ad informare tempestivamente il Titolare del trattamento, fornendo adeguato riscontro agli interessati, in nome e per conto del Titolare del trattamento, nei termini previsti dalla Regolamento UE; **oppure>**
- 2)** ad inoltrare tempestivamente, e comunque nel più breve tempo possibile, le istanze al Titolare del Trattamento, supportando quest'ultimo al fine di fornire adeguato riscontro agli interessati nei termini prescritti.
12. Il Responsabile del trattamento informa tempestivamente e, in ogni caso senza ingiustificato ritardo dall'avvenuta conoscenza, il Titolare di ogni violazione di dati personali (cd. *data breach*); tale notifica è accompagnata da ogni documentazione utile, ai sensi degli artt. 33 e 34 del Regolamento UE, per permettere al Titolare del trattamento,

ove ritenuto necessario, di notificare questa violazione all'Autorità Garante per la protezione dei dati personali, entro il termine di 72 ore da quanto il Titolare ne viene a conoscenza; nel caso in cui il Titolare debba fornire informazioni aggiuntive all'Autorità di controllo, il Responsabile *<da valorizzare in alternativa>* sub-Responsabile del trattamento si impegna a supportare il Titolare nell'ambito di tale attività.

13. Il Responsabile del trattamento deve avvisare tempestivamente e senza ingiustificato ritardo il Titolare in caso di ispezioni, di richiesta di informazioni e di documentazione da parte dell'Autorità Garante per la protezione dei dati personali; inoltre, deve assistere il Titolare nel caso di richieste formulate dall'Autorità Garante in merito al trattamento dei dati personali effettuate in ragione del presente contratto.
14. Il Responsabile del trattamento deve comunicare al Titolare del trattamento il nome ed i dati del proprio "Responsabile della protezione dei dati", qualora, in ragione dell'attività svolta, ne abbia designato uno conformemente all'articolo 37 del Regolamento UE; il Responsabile della protezione dei dati personali del Fornitore/Responsabile collabora e si tiene in costante contatto con il Responsabile della protezione dei dati del Titolare.
15. Al termine della prestazione dei servizi oggetto del contratto, il Responsabile, su richiesta del Titolare, si impegna a: i) restituire al Titolare del trattamento i supporti rimovibili eventualmente utilizzati su cui sono memorizzati i dati; ii) distruggere tutte le informazioni registrate su supporto fisso, documentando per iscritto l'adempimento di tale operazione.
16. Il Fornitore si impegna a individuare e a designare per iscritto gli amministratori di sistema mettendo a disposizione dell'Amministrazione l'elenco aggiornato delle nomine.
17. Il Responsabile del trattamento si impegna ad operare adottando tutte le misure tecniche e organizzative, le attività di formazione, informazione e aggiornamento ragionevolmente necessarie per garantire che i Dati Personali, trattati in esecuzione del contratto attuativo, siano precisi, corretti e aggiornati nel corso della durata del trattamento - anche qualora il trattamento consista nella mera custodia o attività di controllo dei dati - eseguito dal Responsabile, o da un sub-Responsabile.
18. Il Responsabile non può trasferire i dati personali verso un paese terzo o un'organizzazione internazionale salvo che non abbia preventivamente ottenuto l'autorizzazione scritta da parte del Titolare.
19. Sarà obbligo del Titolare del trattamento vigilare durante tutta la durata del trattamento, sul rispetto degli obblighi previsti dalle presenti istruzioni e dal Regolamento UE sulla protezione dei dati da parte del Responsabile del trattamento, nonché a supervisionare l'attività di trattamento dei dati personali effettuando audit, ispezioni e verifiche periodiche sull'attività posta in essere dal Responsabile del trattamento.
20. Durante l'esecuzione del Contratto, nell'eventualità di qualsivoglia modifica della normativa in materia di Trattamento dei Dati Personali che generi nuovi requisiti (ivi incluse nuove misure di natura fisica, logica, tecnica, organizzativa, in materia di sicurezza o trattamento dei dati personali), il Responsabile del trattamento si impegna a collaborare - nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse - con il Titolare affinché siano sviluppate, adottate e implementate misure correttive di adeguamento ai nuovi requisiti.
21. Il Responsabile del trattamento manleva e terrà indenne il Titolare da ogni perdita, contestazione, responsabilità, spese sostenute nonché dei costi subiti (anche in termini di danno reputazionale) in relazione anche ad una sola violazione della normativa in materia di Protezione dei Dati Personali e/o della disciplina sulla protezione dei dati personali contenuta nella Convenzione (inclusi gli Allegati) comunque derivata dalla condotta (attiva e/o omissiva) sua e/o dei suoi agenti e/o subappaltatori e/o sub-contraenti e/o sub-fornitori.



**ALLEGATO F – SCHEMA DI CONTRATTO ESECUTIVO – LOTTO 2**

**CLASSIFICAZIONE DEL DOCUMENTO: CONSIP PUBLIC**

**ALLEGATO F**

**ID 2296**

**SCHEMA DI CONTRATTO ESECUTIVO – LOTTO 2**

Classificazione: Consip Public

Gara a procedura aperta per la conclusione di un Accordo Quadro avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni - ID SIGEF 2296

Allegato F - Schema di Contratto Esecutivo – Lotto 2



## INDICE

1.	DEFINIZIONI .....	5
2.	VALORE DELLE PREMESSE E DEGLI ALLEGATI.....	5
3.	OGGETTO DEL Contratto esecutivo .....	5
4.	EFFICACIA E DURATA.....	6
5.	GESTIONE DEL CONTRATTO ESECUTIVO .....	7
6.	PRESA IN CARICO E TRASFERIMENTO DEL KNOW HOW .....	7
7.	LOCALI MESSI A DISPOSIZIONE DALL'AMMINISTRAZIONE CONTRAENTE .....	7
8.	VERIFICHE DI CONFORMITA' .....	8
9.	PENALI .....	8
10.	CORRISPETTIVI .....	8
11.	FATTURAZIONE E PAGAMENTI .....	8
12.	GARANZIA DELL'ESATTO ADEMPIMENTO .....	9
13.	SUBAPPALTO <i>&lt;ove previsto&gt;</i> .....	11
14.	<i>&lt;EVENTUALE&gt;</i> CONDIZIONI E TEST RICHIESTI DAL CVCN.....	13
15.	RISOLUZIONE E RECESSO.....	13
16.	FORZA MAGGIORE .....	13
17.	RESPONSABILITA' CIVILE <i>&lt;eventuale&gt;</i> E POLIZZA ASSICURATIVA .....	14
18.	TRASPARENZA DEI PREZZI .....	14
19.	ONERI FISCALI E SPESE CONTRATTUALI.....	15
20.	TRACCIABILITÀ DEI FLUSSI FINANZIARI.....	16
21.	FORO COMPETENTE .....	16
22.	TRATTAMENTO DEI DATI PERSONALI .....	16



## CONTRATTO ESECUTIVO

### TRA

\_\_\_\_\_, con sede in \_\_\_\_\_, Via \_\_\_\_\_, C.F. \_\_\_\_\_, nella persona della persona di \_\_\_\_\_, in qualità di \_\_\_\_\_, giusta i poteri conferitigli da \_\_\_\_\_ in data \_\_\_\_\_ (nel seguito per brevità anche “**Amministrazione**”),

### E

\_\_\_\_\_, sede legale in \_\_\_\_\_, Via \_\_\_\_\_, capitale sociale Euro \_\_\_\_\_, iscritta al Registro delle Imprese di \_\_\_\_\_ al n. \_\_\_\_\_, P. IVA \_\_\_\_\_, domiciliata ai fini del presente atto in \_\_\_\_\_, Via \_\_\_\_\_, in persona del \_\_\_\_\_ e legale rappresentante Dott. \_\_\_\_\_, giusta poteri allo stesso conferiti da \_\_\_\_\_ (nel seguito per brevità anche “**Fornitore**”);

### OPPURE

- \_\_\_\_\_, sede legale in \_\_\_\_\_, Via \_\_\_\_\_, capitale sociale Euro \_\_\_\_\_, iscritta al Registro delle Imprese di \_\_\_\_\_ al n. \_\_\_\_\_, P. IVA \_\_\_\_\_, domiciliata ai fini del presente atto in \_\_\_\_\_, Via \_\_\_\_\_, in persona del \_\_\_\_\_ e legale rappresentante Dott. \_\_\_\_\_, nella sua qualità di impresa mandataria capo-gruppo del Raggruppamento Temporaneo oltre alla stessa la mandante \_\_\_\_\_ con sede legale in \_\_\_\_\_, Via \_\_\_\_\_, capitale sociale Euro \_\_\_\_\_, iscritta al Registro delle Imprese di \_\_\_\_\_ al n. \_\_\_\_\_, P. IVA \_\_\_\_\_, domiciliata ai fini del presente atto in \_\_\_\_\_, via \_\_\_\_\_, e la mandante \_\_\_\_\_, con sede legale in \_\_\_\_\_, Via \_\_\_\_\_, capitale sociale Euro \_\_\_\_\_, iscritta al Registro delle Imprese di \_\_\_\_\_ al n. \_\_\_\_\_, P. IVA \_\_\_\_\_, domiciliata ai fini del presente atto in \_\_\_\_\_, via \_\_\_\_\_, giusta mandato collettivo speciale con rappresentanza autenticato dal notaio in \_\_\_\_\_ dott. \_\_\_\_\_ repertorio n. \_\_\_\_\_; (nel seguito per brevità congiuntamente anche “**Fornitore**” o “**Impresa**”)

### PREMESSO CHE

- (A) l’art. 4, comma 3-quater, del D.L. n. 95/2012, come convertito con modificazioni dalla Legge n. 135/2012, ha stabilito che, per la realizzazione di quanto previsto dall’art. 20 del D.L. n. 83/2012, Consip S.p.A. svolge altresì le attività di centrale di committenza relativamente “ai contratti-quadro ai sensi dell’articolo 1, comma 192, della legge 30 dicembre 2004, n. 311”;
- (B) L’articolo 2, comma 225, Legge 23 dicembre 2009, n. 191, consente a Consip S.p.A. di concludere Accordi Quadro a cui le Stazioni Appaltanti, possono fare ricorso per l’acquisto di beni e di servizi.
- (C) Peraltro, l’utilizzazione dello strumento dell’Accordo Quadro e, quindi, una gestione in forma associata della procedura di scelta del contraente, mediante aggregazione della domanda di più soggetti, consente la razionalizzazione della spesa di beni e servizi, il supporto alla programmazione dei fabbisogni, la semplificazione e standardizzazione delle procedure di acquisto, il conseguimento di economie di scala, una maggiore trasparenza delle procedure di gara, il miglioramento della responsabilizzazione e del controllo della spesa, un incremento della specializzazione delle competenze, una maggiore efficienza nell’interazione fra Amministrazione e mercato e, non ultimo, un risparmio nelle spese di gestione della procedura medesima.

Classificazione: Consip Public

Procedura aperta per la conclusione di un Accordo Quadro avente ad oggetto l’affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni - Lotto 2 - ID SIGEF 2296

Allegato F - Schema di Contratto Esecutivo



- (D) In particolare, in forza di quanto stabilito dall'art. 1, comma 514, della legge 28 dicembre 2015, n.208 (Legge di stabilità 2016), "Ai fini di cui al comma 512," – e quindi per rispondere alle esigenze delle amministrazioni pubbliche e delle società inserite nel conto economico consolidato della pubblica amministrazione, come individuate dall'Istituto nazionale di statistica (ISTAT) ai sensi dell'articolo 1 della legge 31 dicembre 2009, n. 19 – "Consip S.p.A. o il soggetto aggregatore interessato sentita l'Agid per l'acquisizione dei beni e servizi strategici indicati nel Piano triennale per l'informatica nella pubblica amministrazione di cui al comma 513, programma gli acquisti di beni e servizi informatici e di connettività, in coerenza con la domanda aggregata di cui al predetto Piano. [...] Consip SpA e gli altri soggetti aggregatori promuovono l'aggregazione della domanda funzionale all'utilizzo degli strumenti messi a disposizione delle pubbliche amministrazioni su base nazionale, regionale o comune a più amministrazioni".
- (E) L'art. 20, comma 4, del D.L. n. 83/2012, come convertito con modificazioni dalla Legge 7 agosto 2012, n. 134, ha affidato a Consip S.p.A., a decorrere dalla data di entrata in vigore della legge di conversione del decreto medesimo, "le attività amministrative, contrattuali e strumentali già attribuite a DigitPA, ai fini della realizzazione e gestione dei progetti in materia, nel rispetto delle disposizioni del comma 3".
- (F) Ai fini del perseguimento degli obiettivi di cui al citato Piano triennale per l'informatica nella Pubblica Amministrazione, e che in esecuzione di quanto precede, Consip S.p.A., in qualità di stazione appaltante e centrale di committenza, ha indetto con Bando di gara pubblicato nella Gazzetta Ufficiale della Repubblica Italiana n. \_\_\_\_ del \_\_\_\_ e nella Gazzetta Ufficiale dell'Unione Europea n. \_\_\_\_ del \_\_\_\_, una procedura aperta per la stipula di un Accordo Quadro per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni, ai sensi dell'art. 54, comma 4, lett. a) del D. Lgs. n. 50/2016, con più operatori.
- (G) Il Fornitore è risultato aggiudicatario della quota PAL del Lotto 2 della predetta gara, ed ha stipulato il relativo Accordo Quadro in data \_\_\_\_\_.
- (H) In applicazione di quanto stabilito nel predetto Accordo Quadro, ciascuna Amministrazione Contraente utilizza il medesimo per la stipula di Contratti esecutivi, secondo quanto disciplinato nell'Accordo Quadro stesso.
- (I) L'Amministrazione Contraente ha svolto ogni attività prodromica necessaria alla stipula del presente Contratto esecutivo, in conformità alle previsioni di cui al Capitolato Tecnico Generale.
- (J) Il Fornitore dichiara che quanto risulta dall'Accordo Quadro e dai suoi allegati, ivi compreso il Capitolato d'Oneri ed il Capitolato Tecnico (Generale e Speciale) dell'Accordo Quadro, nonché dal presente Contratto esecutivo e dai suoi allegati, definisce in modo adeguato e completo gli impegni assunti con la firma del presente Contratto, nonché l'oggetto dei prodotti e dei servizi connessi da fornire e, in ogni caso, che ha potuto acquisire tutti gli elementi per una idonea valutazione tecnica ed economica degli stessi e per la formulazione dell'offerta che ritiene pienamente remunerativa;
- (K) il CIG del presente Contratto Esecutivo è il seguente: \_\_\_\_\_;
- (L) *<ove obbligatorio ai sensi dell'art. 11 della Legge 16 gennaio 2003 n. 3>* il CUP (Codice Unico Progetto) del presente Contratto Esecutivo è il seguente: \_\_\_\_\_;

Classificazione: Consip Public

Procedura aperta per la conclusione di un Accordo Quadro avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni - Lotto 2 - ID SIGEF 2296

Allegato F - Schema di Contratto Esecutivo





## **TUTTO CIÒ PREMESSO SI CONVIENE E SI STIPULA QUANTO SEGUE:**

### **1. DEFINIZIONI**

- 1.1 I termini contenuti nel presente Contratto esecutivo hanno il significato specificato nell'Accordo Quadro e nei relativi Allegati, salvo che il contesto delle singole clausole disponga diversamente.
- 1.2 I termini tecnici contenuti nel presente Contratto esecutivo hanno il significato specificato nel Capitolato Tecnico Generale e Speciale, salvo che il contesto delle singole clausole disponga diversamente.
- 1.3 Il presente Contratto esecutivo è regolato:
- a) dalle disposizioni del presente atto e dai suoi allegati, che costituiscono la manifestazione integrale di tutti gli accordi intervenuti tra il Fornitore e l'Amministrazione relativamente alle attività e prestazioni contrattuali;
  - b) dalle disposizioni dell'Accordo Quadro e dai suoi allegati;
  - c) dalle disposizioni del D.Lgs. 50/2016 e s.m.i. e relative prassi e disposizioni attuative;
  - d) dalle disposizioni di cui al D.Lgs. n. 82/2005;
  - e) dal codice civile e dalle altre disposizioni normative in vigore in materia di contratti di diritto privato.

### **2. VALORE DELLE PREMESSE E DEGLI ALLEGATI**

- 2.1 Le premesse di cui sopra, gli atti e i documenti richiamati nelle medesime premesse e nella restante parte del presente atto, ancorché non materialmente allegati, costituiscono parte integrante e sostanziale del presente Contratto esecutivo.
- 2.2 Costituiscono, altresì, parte integrante e sostanziale del presente Contratto esecutivo:
- l'Accordo Quadro,
  - gli Allegati dell'Accordo Quadro,
  - l'**Allegato 1** "Piano Operativo" approvato, l'**Allegato 2** "Piano dei Fabbisogni", di cui al paragrafo 6.5 del Capitolato Tecnico Parte Generale (Allegato all'Accordo Quadro).
- 2.3 In particolare, per ogni condizione, modalità e termine per la prestazione dei servizi oggetto del presente Contratto Esecutivo che non sia espressamente regolata nel presente atto, vale tra le Parti quanto stabilito nell'Accordo Quadro, ivi inclusi gli Allegati del medesimo, con il quale devono intendersi regolati tutti i termini del rapporto tra le Parti.
- 2.4 Le Parti espressamente convengono che il predetto Accordo Quadro, ha valore di regolamento e pattuizione per il presente Contratto esecutivo. Pertanto, in caso di contrasto tra i principi dell'Accordo Quadro e quelli del Contratto esecutivo, i primi prevarranno su questi ultimi, salvo diversa espressa volontà derogativa delle parti manifestata per iscritto.

### **3. OGGETTO DEL CONTRATTO ESECUTIVO**

- 3.1 Il presente Contratto esecutivo definisce i termini e le condizioni che, unitamente alle disposizioni contenute nell'Accordo Quadro, regolano la prestazione in favore



dell'Amministrazione da parte del Fornitore dei seguenti servizi: \_\_\_\_\_, come riportati nel Piano Operativo approvato di cui all'Allegato 1 e nel Piano dei Fabbisogni di cui all'Allegato 2 al presente documento.

- 3.2 I predetti servizi dovranno essere erogati con le modalità ed alle condizioni stabilite nel presente Contratto esecutivo e nell'Accordo Quadro e relativi allegati.
- 3.3 È designato quale Responsabile unico del procedimento ai sensi dell'art. 31 del D.Lgs. n. 50/2016 e Direttore dell'esecuzione, ai sensi dell'art. 101 del D. Lgs. n. 50/2016, il Dott. \_\_\_\_\_. *<in alternativa: Sono designati quale Responsabile unico del procedimento, ai sensi dell'art. 31 del D. Lgs. n. 50/2016 il Dott. \_\_\_\_\_ e Direttore dell'esecuzione ai sensi dell'art. 101 del D. Lgs. n. 50/2016 il Dott. \_\_\_\_\_>.*
- 3.4 L'affidatario si impegna a rispettare tutti i requisiti tecnici e ambientali previsti dalla normativa europea e nazionale in ottemperanza al principio di non arrecare un danno significativo all'ambiente "Do No Significant Harm" (DNSH), ivi incluso l'impegno a consegnare all'Amministrazione la documentazione a comprova del rispetto dei suddetti requisiti.
- 3.5 *<In caso di Contratto esecutivo affidato da un Soggetto Aggregatore, indicare tutte le singole Amministrazioni per le quali il Soggetto Aggregatore effettua l'Affidamento>.*

#### **4. EFFICACIA E DURATA**

- 4.1 Il presente Contratto esecutivo spiega i suoi effetti dalla data della sua sottoscrizione ed avrà termine allo spirare di \_\_\_\_\_ *<indicare la durata contrattuale in ragione di quanto previsto al par. 2 del Capitolato Tecnico Generale>* mesi dalla data di conclusione delle attività di presa in carico.
- 4.2 Le Amministrazioni possono, nei limiti di quanto previsto all'art. 106, comma 7, del D. Lgs. n. 50/2016, chiedere al Fornitore prestazioni supplementari rispetto al Contratto esecutivo, che si rendano necessarie, ove un cambiamento del contraente produca entrambi gli effetti di cui all'art. 106, comma 1, lettera b), D. Lgs. n. 50/2016; l'Amministrazione comunicherà ad ANAC tale modifica entro i termini di cui all'art. 106, comma 8, del medesimo decreto.
- 4.3 Le Amministrazioni possono apportare modifiche al contratto esecutivo ove siano soddisfatte tutte le condizioni di cui all'art. 106, comma 1, lettera c), D. Lgs. 50/2016, fatto salvo quanto previsto all'art. 106, comma 7, del D. Lgs. n. 50/2016. Al ricorrere delle condizioni di cui all'art. 106, comma 14, del D. Lgs. 50/2016 l'Amministrazione comunicherà ad ANAC tale modifica entro i termini e con le modalità ivi indicati. In entrambi i casi sopra descritti, l'Amministrazione eseguirà le pubblicazioni prescritte dall'art. 106, comma 5, del D. Lgs. n. 50/2016.
- 4.4 Le Amministrazioni potranno apportare le modifiche di cui art. 106, comma 1, lett. d), del D. Lgs. n. 50/2016, nel pieno rispetto di tale previsione normativa.
- 4.5 Ai sensi dell'art. 106, comma 12, del D.Lgs. n. 50/2016, ove ciò si renda necessario in corso di esecuzione, l'Amministrazione potrà imporre al Fornitore affidatario del Contratto esecutivo un aumento o una diminuzione delle prestazioni fino a concorrenza di un quinto dell'importo del contratto alle stesse condizioni ed agli stessi prezzi unitari previsti nel presente contratto. In tal caso, il Fornitore non può far valere il diritto alla risoluzione del contratto.

Classificazione: Consip Public

Procedura aperta per la conclusione di un Accordo Quadro avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni - Lotto 2 - ID SIGEF 2296

Allegato F - Schema di Contratto Esecutivo



## **5. GESTIONE DEL CONTRATTO ESECUTIVO**

- 5.1 Ai fini dell'esecuzione del presente Contratto esecutivo, il Fornitore ha nominato come Responsabile Unico delle Attività Contrattuali (RUAC) e come Referente/i Tecnico/i per l'erogazione dei servizi: il/i dott. \_\_\_\_\_
- 5.2 I compiti demandati alle suddette figure del Fornitore sono declinati al paragrafo 7.2 del Capitolato Tecnico Generale dell'Accordo Quadro.
- 5.3 Le attività di supervisione e controllo della corretta esecuzione del presente Contratto esecutivo, in relazione ai servizi richiesti, sono svolte dall'Amministrazione, eventualmente d'intesa con i soggetti indicati nell'Allegato Governance al Capitolato Tecnico Generale dell'Accordo Quadro.

## **6. PRESA IN CARICO E TRASFERIMENTO DEL KNOW HOW**

- 6.1 Il Fornitore, a decorrere dalla data di stipula del presente Contratto esecutivo, dovrà procedere alla attività di presa in carico con le modalità indicate nel Capitolato Tecnico Speciale dell'Accordo Quadro.
- 6.2 L'attivazione dei servizi avverrà nei tempi e nei modi di cui al Capitolato Tecnico Generale e Speciale dell'Accordo Quadro, al Piano dei Fabbisogni ed al Piano Operativo.
- 6.3 In base ai servizi richiesti da parte dell'Amministrazione contraente, alla scadenza del presente Contratto esecutivo o in caso di risoluzione o recesso dallo stesso, il Fornitore si impegna a porre in essere tutte le attività per il passaggio di consegne di fine fornitura (phase-out), finalizzato al trasferimento all'Amministrazione, o a terzi da essa indicati, del know-how e delle competenze maturate nella conduzione delle attività, secondo quanto previsto nel paragrafo 4.3 del Capitolato Tecnico Speciale (2B).

## **7. LOCALI MESSI A DISPOSIZIONE DALL'AMMINISTRAZIONE CONTRAENTE**

- 7.1 L'Amministrazione Contraente provvede ad indicare e mettere a disposizione del Fornitore, in comodato gratuito ed in uso non esclusivo, locali idonei alla installazione degli eventuali apparati del Fornitore necessari all'erogazione dei servizi richiesti, con le modalità indicate nel Piano dei Fabbisogni e nel Piano Operativo.
- 7.2 L'Amministrazione Contraente garantisce al Fornitore:
- lo spazio fisico necessario per l'alloggio delle apparecchiature ed idoneo ad ospitare le apparecchiature medesime;
  - l'alimentazione elettrica delle apparecchiature di adeguata potenza; sarà cura del Fornitore provvedere ad adottare ogni misura per la garantire la continuità della alimentazione elettrica.
- 7.3 Il Fornitore provvede a visitare i locali messi a disposizione dall'Amministrazione Contraente ed a segnalare, prima della data di disponibilità all'attivazione, l'eventuale inidoneità tecnica degli stessi.
- 7.4 L'Amministrazione Contraente consentirà al personale del Fornitore o a soggetti da esso indicati, muniti di documento di riconoscimento, l'accesso ai propri locali per eseguire eventuali operazioni rientranti nell'oggetto del presente Contratto esecutivo. Le modalità dell'accesso saranno concordate fra le Parti al fine di salvaguardare la legittima esigenza



di sicurezza dell'Amministrazione Contraente. Il Fornitore è tenuto a procedere allo sgombero, a lavoro ultimato, delle attrezzature e dei materiali residui.

- 7.5 L'Amministrazione Contraente, successivamente all'esito positivo delle verifiche di conformità a fine contratto, porrà in essere quanto possibile affinché gli apparati del Fornitore presenti nei suoi locali non vengano danneggiati o manomessi, pur non assumendosi responsabilità se non quelle derivanti da dolo o colpa grave del proprio personale.

## **8. VERIFICHE DI CONFORMITA'**

- 8.1 Nel periodo di efficacia del presente Contratto esecutivo, ciascuna Amministrazione Contraente procederà ad effettuare la verifica di conformità delle prestazioni oggetto di ciascun Contratto esecutivo per la verifica della corretta esecuzione delle prestazioni contrattuali, con le modalità e le specifiche stabilite nell'Accordo Quadro e nel Capitolato Tecnico Generale e Speciale ad esso allegati.

## **9. PENALI**

- 9.1 L'Amministrazione potrà applicare al Fornitore le penali dettagliatamente descritte e regolate nell'Accordo Quadro, qui da intendersi integralmente trascritte.
- 9.2 Per le modalità di contestazione ed applicazione delle penali vale tra le Parti quanto stabilito all'articolo 12 dell'Accordo Quadro.

## **10. CORRISPETTIVI**

- 10.1 Il corrispettivo complessivo, calcolato sulla base del dimensionamento dei servizi indicato del Piano dei Fabbisogni e nel Piano Operativo, è pari a *<inserire importo in cifre>* € \_\_\_\_\_, *<eventuale>* così suddiviso \_\_\_\_\_.
- 10.2 I corrispettivi unitari per singolo servizio, dovuti al Fornitore per la fornitura dei servizi prestati in esecuzione del presente Contratto esecutivo sono determinati in ragione dei prezzi unitari stabiliti nell'Allegato "C" all'Accordo Quadro "Corrispettivi e Tariffe".
- 10.3 Il corrispettivo contrattuale si riferisce alla esecuzione dei servizi a perfetta regola d'arte e nel pieno adempimento delle modalità e delle prescrizioni contrattuali.  
*<nel caso di Contratto Esecutivo affidato da un Soggetto Aggregatore, dovranno essere indicati gli importi e i quantitativi relativi ad ogni singola Amministrazione>*
- 10.4 I corrispettivi contrattuali sono stati determinati a proprio rischio dal Fornitore in base ai propri calcoli, alle proprie indagini, alle proprie stime, e sono, pertanto, fissi ed invariabili indipendentemente da qualsiasi imprevisto o eventualità, facendosi carico il Fornitore medesimo di ogni relativo rischio e/o alea. Il Fornitore non potrà vantare diritto ad altri compensi, ovvero ad adeguamenti, revisioni o aumenti dei corrispettivi come sopra indicati.
- 10.5 Tali corrispettivi sono dovuti dall'Amministrazione Contraente al Fornitore a decorrere dalla "Data di accettazione" della fornitura e successivamente all'esito positivo della verifica di conformità della singola prestazione.

## **11. FATTURAZIONE E PAGAMENTI**

- 11.1 La fattura relativa ai corrispettivi maturati secondo quanto previsto al precedente art. 10

Classificazione: Consip Public

Procedura aperta per la conclusione di un Accordo Quadro avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni - Lotto 2 - ID SIGEF 2296

Allegato F - Schema di Contratto Esecutivo



viene emessa ed inviata dal Fornitore con cadenza \_\_\_\_\_.

- 11.2 Ciascuna fattura dovrà essere emessa nel rispetto di quanto prescritto nell'Accordo Quadro.

*<nel caso di Contratto Esecutivo affidato da un Soggetto Aggregatore, dovranno essere indicate le eventuali modalità di ripartizione degli obblighi di fatturazione tra il Soggetto Aggregatore e le singole Amministrazioni>*

- 11.3 Nel caso in cui risulti aggiudicatario del Contratto un R.T.I., le singole Società costituenti il Raggruppamento, salva ed impregiudicata la responsabilità solidale delle società raggruppate nei confronti dell'Amministrazione, potranno provvedere ciascuna alla fatturazione "pro quota" delle attività effettivamente prestate. Le Società componenti il Raggruppamento potranno fatturare solo le attività effettivamente svolte, corrispondenti alla ripartizione delle attività. La società mandataria del Raggruppamento medesimo è obbligata a trasmettere, in maniera unitaria e previa predisposizione di apposito prospetto riepilogativo delle attività e delle competenze maturate, le fatture relative all'attività svolta da tutte le imprese raggruppate. Ogni singola fattura dovrà contenere la descrizione di ciascuno dei servizi / attività / fasi / prodotti a cui si riferisce.
- 11.4 I corrispettivi saranno accreditati, a spese del Fornitore, sul conto corrente n. \_\_\_\_\_, intestato al Fornitore presso \_\_\_\_\_, Codice IBAN \_\_\_\_\_; il Fornitore dichiara che il predetto conto opera nel rispetto della Legge 13 agosto 2010 n. 136 e si obbliga a comunicare le generalità e il codice fiscale del/i delegato/i ad operare sul/i predetto/i conto/i all'Amministrazione all'atto del perfezionamento del presente Contratto Esecutivo.
- 11.5 Ove applicabile in funzione della tipologia di prestazioni, ai sensi dell'art. 35, comma 18, del Codice, così come novellato dal D.L. 32/2019, il fornitore può ricevere, entro 15 giorni dall'effettivo inizio della/e prestazione/i contrattuali un'anticipazione del prezzo di ciascun Contratto Esecutivo pari al 20 per cento del valore del Contratto Esecutivo stesso. L'erogazione dell'anticipazione è subordinata alla costituzione di una garanzia fideiussoria bancaria o assicurativa in favore dell'Amministrazione Contraente beneficiaria della prestazione, rilasciata dai soggetti indicati all'art. 35, comma 18, del Codice, di importo pari all'anticipazione, maggiorato del tasso di interesse legale applicato al periodo necessario al recupero dell'anticipazione stessa secondo il cronoprogramma (o altro documento equivalente tipo SLA) della prestazione che indicato nel Capitolato Tecnico relativo all'Appalto Specifico
- 11.6 L'importo della garanzia viene gradualmente ed automaticamente ridotto nel corso dello svolgimento della/e prestazione/i, in rapporto al progressivo recupero dell'anticipazione da parte delle Amministrazioni.
- 11.7 Il Fornitore decade dall'anticipazione, con obbligo di restituzione delle somme anticipate, se l'esecuzione della/e prestazione/i, non procede, per ritardi a lui imputabili, secondo il cronoprogramma concordato. Sulle somme restituite sono dovuti gli interessi legali con decorrenza dalla data di erogazione dell'anticipazione.

## **12. GARANZIA DELL'ESATTO ADEMPIMENTO**

- 12.1 Il Fornitore ha prestato garanzia definitiva rilasciata in data \_\_\_\_\_ dalla \_\_\_\_\_ avente n. \_\_\_\_\_ di importo pari ad Euro \_\_\_\_\_ = (\_\_\_\_\_/00) che copre le

Classificazione: Consip Public

Procedura aperta per la conclusione di un Accordo Quadro avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni - Lotto 2 - ID SIGEF 2296

Allegato F - Schema di Contratto Esecutivo



obbligazioni assunte con il presente contratto, il risarcimento dei danni derivanti dall'eventuale inadempimento delle stesse obbligazioni, nonché il rimborso delle somme pagate in più all'esecutore rispetto alle risultanze della liquidazione finale, salva comunque la risarcibilità del maggior danno verso l'appaltatore, nonché, ove esistente, le obbligazioni assunte con il Patto di integrità.

- 12.2 L'Amministrazione ha inoltre il diritto di valersi della garanzia definitiva, nei limiti dell'importo massimo garantito: i) per l'eventuale maggiore spesa sostenuta per il completamento delle prestazioni nel caso di risoluzione del contratto disposta in danno dell'esecutore; ii) per provvedere al pagamento di quanto dovuto dal Fornitore per le inadempienze derivanti dalla inosservanza di norme e prescrizioni dei contratti collettivi, delle leggi e dei regolamenti sulla tutela, protezione, assicurazione, assistenza e sicurezza fisica dei lavoratori comunque presenti nei luoghi dove viene eseguito il contratto ed addetti all'esecuzione dell'appalto.
- 12.3 L'Amministrazione ha diritto di incamerare la garanzia, in tutto o in parte, per i danni che essa affermi di aver subito, senza pregiudizio dei suoi diritti nei confronti del Fornitore per la rifusione dell'ulteriore danno eventualmente eccedente la somma incamerata.
- 12.4 La garanzia prevede espressamente la rinuncia della preventiva escussione del debitore principale, la rinuncia all'eccezione di cui all'art. 1957, comma 2 del codice civile, nonché l'operatività della garanzia medesima entro 15 giorni, a semplice richiesta scritta.
- 12.5 Il Fornitore si impegna a tenere valida ed efficace la garanzia, mediante rinnovi e proroghe, per tutta la durata del presente contratto e, comunque, sino al perfetto adempimento delle obbligazioni assunte in virtù del presente contratto, pena la risoluzione di diritto del medesimo.
- 12.6 L'Amministrazione può richiedere al Fornitore la reintegrazione della garanzia ove questa sia venuta meno in tutto o in parte entro il termine di 10 (dieci) giorni dalla richiesta; in caso di inottemperanza, l'Amministrazione conseguirà la reintegrazione trattenendo quanto necessario dai corrispettivi dovuti al Fornitore.
- 12.7 La garanzia sarà progressivamente svincolata a misura dell'avanzamento dell'esecuzione contrattuale, nel limite massimo dell'80 per cento dell'iniziale importo garantito, secondo quanto stabilito dall'art. 103, comma 5, del D. Lgs. n. 50/2016, previa deduzione di crediti dell'Amministrazione verso il Fornitore e subordinatamente alla preventiva consegna, da parte del Fornitore all'Istituto garante, di un documento, in originale o copia autentica, attestante l'avvenuta esecuzione delle prestazioni contrattuali. Tale documento è emesso periodicamente dall'Amministrazione in ragione delle verifiche di conformità svolte. Il fornitore dovrà inviare per conoscenza all'Amministrazione la comunicazione che invia al Garante ai fini dello svincolo. Il Garante dovrà comunicare all'Amministrazione il valore dello svincolo. L'Amministrazione si riserva di verificare la correttezza degli importi svincolati e di chiedere al Fornitore ed al Garante in caso di errore un'integrazione.
- 12.8 L'ammontare residuo della garanzia definitiva deve permanere fino alla data di emissione del certificato di verifica di conformità attestante la corretta esecuzione del Contratto esecutivo.
- 12.9 Resta fermo tutto quanto previsto dall'art. 103 del D. Lgs. n. 50/2016.





**13. SUBAPPALTO <OVE PREVISTO>**

- 13.1 L'Impresa si è riservata di affidare in subappalto, nella misura di \_\_\_\_\_, l'esecuzione delle seguenti prestazioni: \_\_\_\_\_, salvo quanto previsto dall'art. 105, comma 12, del d. lgs. n. 50/2016.
- 13.2 L'Impresa si impegna a depositare presso Consip S.p.A., almeno venti giorni prima della data di effettivo inizio dell'esecuzione delle attività oggetto del subappalto: i) l'originale o la copia autentica del contratto di subappalto che deve indicare puntualmente l'ambito operativo del subappalto sia in termini prestazionali che economici; ii) dichiarazione attestante il possesso da parte del subappaltatore dei requisiti richiesti dalla documentazione di gara, per lo svolgimento delle attività allo stesso affidate, ivi inclusi i requisiti di ordine generale di cui all'articolo 80 del D. Lgs. n. 50/2016; iii) dichiarazione dell'appaltatore relativa alla sussistenza o meno di eventuali forme di controllo o collegamento a norma dell'art. 2359 c.c. con il subappaltatore; se del caso, v) documentazione attestante il possesso da parte del subappaltatore dei requisiti di qualificazione/certificazione prescritti dal D. Lgs. n. 50/2016 per l'esecuzione delle attività affidate.
- 13.3 In caso di mancato deposito di taluno dei suindicati documenti nel termine all'uopo previsto, Consip S.p.A. procederà a richiedere al Fornitore l'integrazione della suddetta documentazione. Resta inteso che la suddetta richiesta di integrazione comporta l'interruzione del termine per la definizione del procedimento di autorizzazione del subappalto, che ricomincerà a decorrere dal completamento della documentazione.
- 13.4 I subappaltatori dovranno mantenere per tutta la durata del presente contratto, i requisiti richiesti per il rilascio dell'autorizzazione al subappalto. In caso di perdita dei detti requisiti Consip S.p.A. revocherà l'autorizzazione.
- 13.5 L'impresa qualora l'oggetto del subappalto subisca variazioni e l'importo dello stesso sia incrementato nonché siano variati i requisiti di qualificazione o le certificazioni deve acquisire una autorizzazione integrativa.
- 13.6 Ai sensi dell'art. 105, comma 4, lett. a) del D. Lgs. n. 50/2016 e s.m.i. non sarà autorizzato il subappalto ad un operatore economico che abbia partecipato alla procedura di affidamento dell'Accordo Quadro.
- 13.7 Per le prestazioni affidate in subappalto: il subappaltatore, ai sensi dell'art. 105, comma 14, del Codice, deve garantire gli stessi standard qualitativi e prestazionali previsti nel contratto di appalto e riconoscere ai lavoratori un trattamento economico e normativo non inferiore a quello che avrebbe garantito il contraente principale, inclusa l'applicazione dei medesimi contratti collettivi nazionali di lavoro, qualora le attività oggetto di subappalto coincidano con quelle caratterizzanti l'oggetto dell'appalto ovvero riguardino le lavorazioni relative alle categorie prevalenti e siano incluse nell'oggetto sociale del contraente principale;
- 13.8 L'Amministrazione contraente, sentito il direttore dell'esecuzione, provvede alla verifica dell'effettiva applicazione degli obblighi di cui al presente comma. Il Fornitore è solidalmente responsabile con il subappaltatore degli adempimenti, da parte di questo ultimo, degli obblighi di sicurezza previsti dalla normativa vigente.



- 13.9 Il Fornitore e il subappaltatore sono responsabili in solido, nei confronti dell'Amministrazione Contraente, in relazione alle prestazioni oggetto del contratto di subappalto.
- 13.10 L'Impresa è responsabile in solido con il subappaltatore nei confronti dell'Amministrazione contraente dei danni che dovessero derivare ad essa o a terzi per fatti comunque imputabili ai soggetti cui sono state affidate le suddette attività. In particolare, il Fornitore e il subappaltatore si impegnano a manlevare e tenere indenne la Consip e l'Amministrazione da qualsivoglia pretesa di terzi per fatti e colpe imputabili al subappaltatore o ai suoi ausiliari derivanti da qualsiasi perdita, danno, responsabilità, costo o spesa che possano originarsi da eventuali violazioni del Regolamento 679/2016.
- 13.11 Il Fornitore è responsabile in solido dell'osservanza del trattamento economico e normativo stabilito dai contratti collettivi nazionale e territoriale in vigore per il settore e per la zona nella quale si eseguono le prestazioni da parte del subappaltatore nei confronti dei suoi dipendenti, per le prestazioni rese nell'ambito del subappalto. Il Fornitore trasmette all'Amministrazione contraente prima dell'inizio delle prestazioni la documentazione di avvenuta denuncia agli enti previdenziali, inclusa la Cassa edile, ove presente, assicurativi e antinfortunistici, nonché copia del piano della sicurezza di cui al D. Lgs. n. 81/2008. Ai fini del pagamento delle prestazioni rese nell'ambito dell'appalto o del subappalto, la stazione appaltante acquisisce d'ufficio il documento unico di regolarità contributiva in corso di validità relativo a tutti i subappaltatori.
- 13.12 Il Fornitore è responsabile in solido con il subappaltatore in relazione agli obblighi retributivi e contributivi, ai sensi dell'art. 29 del D. Lgs. n. 276/2003, ad eccezione del caso in cui ricorrano le fattispecie di cui all'art. 105, comma 13, lett. a) e c), del D. Lgs. n. 50/2016.
- 13.13 Il Fornitore si impegna a sostituire i subappaltatori relativamente ai quali apposita verifica abbia dimostrato la sussistenza dei motivi di esclusione di cui all'articolo 80 del D. Lgs. n. 50/2016.
- 13.14 L'Amministrazione Contraente corrisponde direttamente al subappaltatore, al cottimista, al prestatore di servizi ed al fornitore di beni o lavori, l'importo dovuto per le prestazioni dagli stessi eseguite nei seguenti casi: a) quando il subappaltatore o il cottimista è una microimpresa o piccola impresa; b) in caso di inadempimento da parte dell'appaltatore; c) su richiesta del subappaltatore e se la natura del contratto lo consente. In caso contrario, salvo diversa indicazione del direttore dell'esecuzione, il Fornitore si obbliga a trasmettere all'Amministrazione contraente entro 20 giorni dalla data di ciascun pagamento da lui effettuato nei confronti dei subappaltatori, copia delle fatture quietanzate relative ai pagamenti da essa via via corrisposte al subappaltatore.
- 13.15 L'esecuzione delle attività subappaltate non può formare oggetto di ulteriore subappalto.
- 13.16 In caso di inadempimento da parte dell'Impresa agli obblighi di cui ai precedenti commi, l'Amministrazione può risolvere il Contratto esecutivo, salvo il diritto al risarcimento del danno.
- 13.17 Ai sensi dell'art. 105, comma 2, del D. Lgs. n. 50/2016, il Fornitore si obbliga a comunicare all'Amministrazione il nome del subcontraente, l'importo del contratto, l'oggetto delle prestazioni affidate.



- 13.18 Il Fornitore si impegna a comunicare all'Amministrazione, prima dell'inizio della prestazione, per tutti i sub-contratti che non sono subappalti, stipulati per l'esecuzione del contratto, il nome del sub-contraente, l'importo del sub-contratto, l'oggetto del lavoro, servizio o fornitura affidati. Sono, altresì, comunicate eventuali modifiche a tali informazioni avvenute nel corso del sub-contratto.
- 13.19 Non costituiscono subappalto le fattispecie di cui al comma 3 dell'art. 105 del d. lgs. n. 50/2016 e s.m.i.. Nel caso in cui l'Impresa intenda ricorrere alle prestazioni di soggetti terzi in forza di contratti continuativi di cooperazione, servizio e/o fornitura gli stessi devono essere stati sottoscritti in epoca anteriore all'indizione della procedura finalizzata all'aggiudicazione del contratto e devono essere consegnati all'Amministrazione prima o contestualmente alla sottoscrizione del Contratto.
- 13.20 Per tutto quanto non previsto si applicano le disposizioni di cui all'art. 105 del D.Lgs. 50/2016.
- 13.21 Restano fermi tutti gli obblighi e gli adempimenti previsti dall'art. 48-bis del D.P.R. 602 del 29 settembre 1973 nonché dai successivi regolamenti.
- 13.22 L'Amministrazione provvederà a comunicare al Casellario Informativo le informazioni di cui alla Determinazione dell'Autorità di Vigilanza sui Contratti Pubblici (ora A.N.AC) n. 1 del 10/01/2008.

#### **14. <EVENTUALE> CONDIZIONI E TEST RICHIESTI DAL CVCN**

*<Eventuale inserire condizioni/test in considerazione del riscontro del CVCN ai sensi dell'art. 1, comma 6, Legge n. 133/2019>*

#### **15. RISOLUZIONE E RECESSO**

- 15.1 Le ipotesi di risoluzione del presente Contratto esecutivo e di recesso sono disciplinate, rispettivamente, agli artt. 14 e 15 dell'Accordo Quadro, cui si rinvia, nonché agli artt. "SUBAPPALTO" "TRASPARENZA DEI PREZZI", "TRACCIABILITÀ DEI FLUSSI FINANZIARI" e "TRATTAMENTO DEI DATI PERSONALI" del presente Documento.
- 15.2 *<Eventuale inserire le ipotesi di risoluzione o sospensione in accordo con quanto previsto nel precedente articolo 14>*

#### **16. FORZA MAGGIORE**

- 16.1 Nessuna Parte sarà responsabile per qualsiasi perdita che potrà essere patita dall'altra Parte a causa di eventi di forza maggiore (che includono, a titolo esemplificativo, disastri naturali, terremoti, incendi, fulmini, guerre, sommosse, sabotaggi, atti del Governo, autorità giudiziarie, autorità amministrative e/o autorità di regolamentazione indipendenti) a tale Parte non imputabili.
- 16.2 Nel caso in cui un evento di forza maggiore impedisca la prestazione dei servizi da parte del Fornitore, l'Amministrazione, impeggiando qualsiasi diritto ad essa spettante in base alle disposizioni di legge sull'impossibilità della prestazione, non dovrà pagare i corrispettivi per la prestazione dei servizi fino a che i servizi non siano ripristinati e, ove

Classificazione: Consip Public

Procedura aperta per la conclusione di un Accordo Quadro avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni - Lotto 2 - ID SIGEF 2296

Allegato F - Schema di Contratto Esecutivo



possibile, avrà diritto di affidare l'erogazione dei servizi in questione ad altro fornitore assegnatario per una durata ragionevole secondo le circostanze.

- 16.3 L'Amministrazione si impegna, inoltre, in tale eventualità a compiere le azioni necessarie al fine di risolvere tali accordi, non appena il Fornitore le comunichi di essere in grado di erogare nuovamente i servizi.

## **17. RESPONSABILITA' CIVILE *<eventuale>* E POLIZZA ASSICURATIVA**

- 17.1 Fermo restando quanto previsto dall'Accordo Quadro, il Fornitore assume in proprio ogni responsabilità per infortunio o danni eventualmente subiti da parte di persone o di beni, tanto del Fornitore quanto dell'Amministrazione o di terzi, in dipendenza di omissioni, negligenze o altre inadempienze attinenti all'esecuzione delle prestazioni contrattuali ad esso riferibili, anche se eseguite da parte di terzi.

### ***<ove prevista>***

- 17.2 A fronte dell'obbligo di cui al precedente comma, il Fornitore ha presentato polizza/e assicurativa/e conforme/i ai requisiti indicati nella Richiesta di Offerta (conformi all'allegato di gara dell'AQ).
- 17.3 Resta ferma l'intera responsabilità del Fornitore anche per danni coperti o non coperti e/o per danni eccedenti i massimali assicurati dalle polizze di cui al precedente comma 2.
- 17.4 Con specifico riguardo al mancato pagamento del premio, ai sensi dell'art. 1901 del c.c., l'Amministrazione si riserva la facoltà di provvedere direttamente al pagamento dello stesso, entro un periodo di 60 giorni dal mancato versamento da parte del Fornitore ferma restando la possibilità dell'Amministrazione di procedere a compensare quanto versato con i corrispettivi maturati a fronte delle attività eseguite.
- 17.5 Qualora il Fornitore non sia in grado di provare in qualsiasi momento la piena operatività delle coperture assicurative di cui al precedente comma 2 e qualora l'Amministrazione non si sia avvalsa della facoltà di cui al precedente comma 4, il Contratto potrà essere risolto di diritto con conseguente ritenzione della garanzia prestata a titolo di pena le e fatto salvo l'obbligo di risarcimento del maggior danno subito.
- 17.6 Resta fermo che il Fornitore si impegna a consegnare, annualmente e con tempestività, all'Amministrazione, la quietanza di pagamento del premio, atta a comprovare la validità della polizza assicurativa prodotta per la stipula del contratto o, se del caso, la nuova polizza eventualmente stipulata, in relazione al presente contratto.

## **18. TRASPARENZA DEI PREZZI**

- 18.1 L'Impresa espressamente ed irrevocabilmente:
- a) dichiara che non vi è stata mediazione o altra opera di terzi per la conclusione del presente contratto;
  - b) dichiara di non aver corrisposto né promesso di corrispondere ad alcuno, direttamente o attraverso terzi, ivi comprese le Imprese collegate o controllate, somme di denaro o altra utilità a titolo di intermediazione o simili, comunque volte a facilitare la conclusione del contratto stesso;
  - c) si obbliga a non versare ad alcuno, a nessun titolo, somme di danaro o altra utilità finalizzate a facilitare e/o a rendere meno onerosa l'esecuzione e/o la gestione del

Classificazione: Consip Public

Procedura aperta per la conclusione di un Accordo Quadro avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni - Lotto 2 - ID SIGEF 2296

Allegato F - Schema di Contratto Esecutivo



presente contratto rispetto agli obblighi con esse assunti, né a compiere azioni comunque volte agli stessi fini;

- d) si obbliga al rispetto di quanto stabilito dall'art. 42 del D.Lgs. n. 50/2016 al fine di evitare situazioni di conflitto d'interesse.
- 18.2 Qualora non risultasse conforme al vero anche una sola delle dichiarazioni rese ai sensi del precedente comma, o il Fornitore non rispettasse gli impegni e gli obblighi di cui alle lettere c) e d) del precedente comma per tutta la durata del contratto lo stesso si intenderà risolto di diritto ai sensi e per gli effetti dell'art. 1456 cod. civ., per fatto e colpa del Fornitore, che sarà conseguentemente tenuto al risarcimento di tutti i danni derivanti dalla risoluzione e con facoltà della Committente di incamerare la garanzia prestata.

## **19. ONERI FISCALI E SPESE CONTRATTUALI**

- 19.1 Il Fornitore riconosce a proprio carico tutti gli oneri fiscali e tutte le spese contrattuali relative al presente atto, come previsto all'art. 28 dell'Accordo Quadro.
- 19.2 Così come previsto dall'art. 29 del Accordo Quadro, ai sensi dell'art. 4, comma 3-quater, del D.L. 6 luglio 2012, n. 95, convertito con modificazioni in legge 7 agosto 2012, n. 135, si applica il contributo di cui all'art. 18, comma 3, D.Lgs. 1 dicembre 2009, n. 177, come disciplinato dal D.P.C.M. 23 giugno 2010. Pertanto, le Amministrazioni Beneficiarie sono tenute a versare a Consip S.p.A., entro il termine di 30 (trenta) giorni solari dalla data di perfezionamento del presente Contratto esecutivo, il predetto contributo nella misura prevista dall'art. 2, lettera a) (8 per mille del valore del contratto esecutivo sottoscritto se non superiore ad € 1.000.000,00) o lettera b) (5 per mille del valore del contratto esecutivo sottoscritto se superiore ad € 1.000.000,00), del D.P.C.M. 23 giugno 2010, in ragione del valore complessivo del presente Contratto Esecutivo.
- 19.3 Il valore complessivo del presente Contratto Esecutivo è quello espressamente indicato al precedente paragrafo 10.1. Di conseguenza, il valore del contributo dovuto dall'Amministrazione Beneficiaria ammonta ad € \_\_\_\_\_ (Euro \_\_\_\_\_).
- 19.4 In caso di incremento (entro il 20% dell'importo iniziale) del valore del Contratto esecutivo a seguito di una modifica del Piano dei Fabbisogni e del Piano Operativo approvato dall'Amministrazione Beneficiaria ai sensi dell'articolo 6 dell'Accordo Quadro, quest'ultima è tenuta a versare a Consip S.p.A., entro il termine di 30 (trenta) giorni solari dalla predetta approvazione, un ulteriore contributo nella misura prevista dall'art. 2, lettera c) (3 per mille sull'incremento tra il valore del contratto esecutivo ed il valore dell'atto aggiuntivo), del D.P.C.M. 23 giugno 2010.
- A tal fine, nei casi di cui al precedente periodo, il Fornitore provvederà a comunicare all'Amministrazione e per conoscenza a Consip, entro il termine di 10 (dieci) giorni solari dalla data di approvazione del Piano Operativo incrementato, il valore aggiornato del Piano Operativo e il valore del contributo dovuto in ragione del relativo incremento.
- 19.5 Il pagamento del contributo, deve essere effettuato tramite bonifico bancario sul seguente IBAN: Banca: Intesa San Paolo - IBAN: IT 27 X 03069 05036 100000004389
- Detti contributi sono considerati fuori campo dell'applicazione dell'IVA, ai sensi dell'art. 2, comma 3, lettera a) del D.P.R. del 1972 e pertanto non è prevista nessuna emissione di fattura; gli stessi non rientrano nell'ambito di applicazione della tracciabilità dei flussi finanziari di cui all'articolo 3 della legge 13 agosto 2010, n. 136.



## **20. TRACCIABILITÀ DEI FLUSSI FINANZIARI**

- 20.1 Ai sensi e per gli effetti dell'art. 3, comma 8, della Legge 13 agosto 2010 n. 136, il Fornitore si impegna a rispettare puntualmente quanto previsto dalla predetta disposizione in ordine agli obblighi di tracciabilità dei flussi finanziari.
- 20.2 Ferme restando le ulteriori ipotesi di risoluzione previste dal presente contratto, si conviene che l'Amministrazione, in ottemperanza a quanto disposto dall'art. 3, comma 9 bis della Legge 13 agosto 2010 n. 136, senza bisogno di assegnare previamente alcun termine per l'adempimento, potrà risolvere di diritto il presente contratto ai sensi dell'art. 1456 cod. civ., nonché ai sensi dell'art. 1360 cod. civ., previa dichiarazione da comunicarsi all'Impresa con raccomandata a/r qualora le transazioni siano eseguite senza avvalersi del bonifico bancario o postale ovvero degli altri strumenti idonei a consentire la piena tracciabilità delle operazioni ai sensi della Legge 13 agosto 2010 n. 136.
- 20.3 Il Fornitore, nella sua qualità di appaltatore, si obbliga, a mente dell'art. 3, comma 8, secondo periodo della Legge 13 agosto 2010 n. 136, ad inserire nei contratti sottoscritti con i subappaltatori o i subcontraenti, a pena di nullità assoluta, un'apposita clausola con la quale ciascuno di essi assume gli obblighi di tracciabilità dei flussi finanziari di cui alla Legge 13 agosto 2010 n. 136.
- 20.4 Il Fornitore, il subappaltatore o il subcontraente che ha notizia dell'inadempimento della propria controparte agli obblighi di tracciabilità finanziaria di cui alla norma sopra richiamata è tenuto a darne immediata comunicazione all'Amministrazione e la Prefettura – Ufficio Territoriale del Governo della provincia ove ha sede l'Amministrazione.
- 20.5 Il Fornitore, si obbliga e garantisce che nei contratti sottoscritti con i subappaltatori e i subcontraenti, verrà assunta dalle predette controparti l'obbligazione specifica di risoluzione di diritto del relativo rapporto contrattuale nel caso di mancato utilizzo del bonifico bancario o postale ovvero degli strumenti idonei a consentire la piena tracciabilità dei flussi finanziari.
- 20.6 L'Impresa è tenuta a comunicare tempestivamente e comunque entro e non oltre 7 giorni dalla/e variazione/i qualsivoglia variazione intervenuta in ordine ai dati relativi agli estremi identificativi del/i conto/i corrente/i dedicato/i nonché le generalità (nome e cognome) e il codice fiscale delle persone delegate ad operare su detto/i conto/i.
- 20.7 Ai sensi della Determinazione dell'AVCP (ora A.N.AC.) n. 10 del 22 dicembre 2010, il Fornitore, in caso di cessione dei crediti, si impegna a comunicare il/i CIG/CUP al cessionario, eventualmente anche nell'atto di cessione, affinché lo/gli stesso/i venga/no riportato/i sugli strumenti di pagamento utilizzati. Il cessionario è tenuto ad utilizzare conto/i corrente/i dedicato/i, nonché ad anticipare i pagamenti al Fornitore mediante bonifico bancario o postale sul/i conto/i corrente/i dedicato/i del Fornitore medesimo riportando il CIG/CUP dallo stesso comunicato.

## **21. FORO COMPETENTE**

- 21.1 Per tutte le questioni relative ai rapporti tra il Fornitore e l'Amministrazione, la competenza è determinata in base alla normativa vigente.

## **22. TRATTAMENTO DEI DATI PERSONALI**

Classificazione: Consip Public

Procedura aperta per la conclusione di un Accordo Quadro avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni - Lotto 2 - ID SIGEF 2296

Allegato F - Schema di Contratto Esecutivo





*<specificare, nella Piano dei Fabbisogni e nei rispettivi documenti allegati, un sufficiente dettaglio sul contesto tecnologico e procedurale nel quale il Fornitore dovrà operare, anche con specifico riferimento alle misure tecniche e organizzative necessarie per garantire il rispetto degli obblighi di cui all'art. 32 del regolamento UE, coordinando tali informazioni con quanto indicato nell'atto di nomina del Fornitore a Responsabile del trattamento >*

- 22.1 Con la sottoscrizione del presente contratto il Fornitore è nominato Responsabile del trattamento ai sensi dell'art. 28 del Regolamento UE n. 2016/679 sulla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (nel seguito anche "Regolamento UE"), per tutta la durata del contratto. A tal fine il Responsabile è autorizzato a trattare i dati personali necessari per l'esecuzione delle attività oggetto del contratto e si impegna ad effettuare, per conto del Titolare, le sole operazioni di trattamento necessarie per fornire il servizio oggetto del presente contratto, nei limiti delle finalità ivi specificate, nel rispetto del Codice Privacy, del Regolamento UE (nel seguito anche "Normativa in tema di trattamento dei dati personali") e delle istruzioni nel seguito fornite.
- 22.2 Il Fornitore/Responsabile ha presentato garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse per l'adozione di misure tecniche ed organizzative adeguate volte ad assicurare che il trattamento sia conforme alle prescrizioni della normativa in tema di trattamento dei dati personali.
- 22.3 Le finalità del trattamento sono: \_\_\_\_\_ (motivi per cui il fornitore tratta i dati)  
*<Valorizzare in ragione dell'oggetto del contratto>*
- 22.4 Il tipo di dati personali trattati in ragione delle attività oggetto del contratto sono: i) dati comuni (es. dati anagrafici e di contatto ecc..); ii) dati sensibili (dati sanitari, opinioni politiche ecc.); iii) dati giudiziari. *<Valorizzare in ragione dell'oggetto del contratto>*
- 22.5 Le categorie di interessati sono: es. dipendenti e collaboratori, utenti dei servizi, ecc...  
*<Valorizzare in ragione dell'oggetto del contratto>*
- 22.6 Nell'esercizio delle proprie funzioni, il Responsabile si impegna a:
- a) rispettare la normativa vigente in materia di trattamento dei dati personali, ivi comprese le norme che saranno emanate nel corso della durata del contratto;
  - b) trattare i dati personali per le sole finalità specificate e nei limiti dell'esecuzione delle prestazioni contrattuali;
  - c) trattare i dati conformemente alle istruzioni impartite dal Titolare e di seguito indicate che il Fornitore si impegna a far osservare anche alle persone da questi autorizzate ad effettuare il trattamento dei dati personali oggetto del presente contratto, d'ora in poi "persone autorizzate"; nel caso in cui ritenga che un'istruzione costituisca una violazione del Regolamento UE sulla protezione dei dati o delle altre disposizioni di legge relative alla protezione dei dati personali, il Fornitore deve informare immediatamente il Titolare del trattamento;
  - d) garantire la riservatezza dei dati personali trattati nell'ambito del presente contratto e verificare che le persone autorizzate a trattare i dati personali in virtù del presente contratto:



- si impegnino a rispettare la riservatezza o siano sottoposti ad un obbligo legale appropriato di segretezza;
  - ricevano la formazione necessaria in materia di protezione dei dati personali;
  - trattino i dati personali osservando le istruzioni impartite dal Titolare per il trattamento dei dati personali al Responsabile del trattamento;
- e) adottare politiche interne e attuare misure che soddisfino i principi della protezione dei dati personali fin dalla progettazione di tali misure (privacy by design), nonché adottare misure tecniche ed organizzative adeguate per garantire che i dati personali siano trattati, in ossequio al principio di necessità ovvero che siano trattati solamente per le finalità previste e per il periodo strettamente necessari o al raggiungimento delle stesse (privacy by default).
- f) valutare i rischi inerenti il trattamento dei dati personali e adottare tutte le misure tecniche ed organizzative che soddisfino i requisiti del Regolamento UE anche al fine di assicurare un adeguato livello di sicurezza dei trattamenti, in modo tale da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, modifica, divulgazione non autorizzata, nonché di accesso non autorizzato, anche accidentale o illegale, o di trattamento non consentito o non conforme alle finalità della raccolta;
- g) su eventuale richiesta del Titolare, assistere quest'ultimo nello svolgimento della valutazione d'impatto sulla protezione dei dati, conformemente all'articolo 35 del Regolamento UE e nella eventuale consultazione del Garante per la protezione dei dati personale, prevista dall'articolo 36 del medesimo Regolamento UE;
- h) ai sensi dell'art. 30 del Regolamento UE, e nei limiti di quanto esso prescrive *< si precisa che tale obbligo non si applica alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato o includa il trattamento di dati sensibili di cui all'articolo 9, paragrafo 1, o i dati giudiziari di cui all'articolo 10 >*, tenere un Registro delle attività di trattamento effettuate sotto la propria responsabilità e cooperare con il Titolare e con l'Autorità Garante per la protezione dei dati personali, mettendo il predetto Registro a disposizione del Titolare e dell'Autorità, laddove ne venga fatta richiesta ai sensi dell'art. 30 comma 4 del Regolamento UE;
- i) assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli artt. da 31 a 36 del Regolamento UE.
- 22.7 Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, il Responsabile del trattamento deve mettere in atto misure tecniche ed organizzative idonee per garantire un livello di sicurezza adeguato al rischio e per garantire il rispetto degli obblighi di cui all'art. 32 del Regolamento UE. Tali misure comprendono tra le altre, se del caso *< personalizzare in ragione dell'oggetto del contratto >*:
- la pseudonimizzazione e la cifratura dei dati personali;
  - la capacità di assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi che trattano i dati personali;



- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

22.8 1) (Autorizzazione generale) Il Responsabile del trattamento può ricorrere ad un altro Responsabile del trattamento (di seguito, "sub-Responsabile del trattamento") per gestire attività di trattamento specifiche, informando, periodicamente il Titolare del trattamento di ogni nomina e/o sostituzione dei Responsabili. Nella comunicazione andranno specificate le attività di trattamento delegate, i dati identificativi del sub-Responsabile del trattamento e i dati del contratto di esternalizzazione.

<Oppure> 2) (Autorizzazione specifica) Il Responsabile del trattamento può avvalersi di ulteriori Responsabili per delegargli attività specifiche, previa autorizzazione scritta del Titolare del trattamento. Nel caso in cui per le prestazioni del Contratto che comportano il trattamento di dati personali il Fornitore/ Responsabile ricorra a subappaltatori o subcontraenti è obbligato a nominare tali operatori a loro volta sub-Responsabili del trattamento sulla base della modalità sopra indicata e comunicare l'avvenuta nomina al titolare.

Il sub-Responsabile del trattamento deve rispettare obblighi analoghi a quelli forniti dal Titolare al Responsabile Iniziale del trattamento, riportate in uno specifico contratto o atto di nomina. Spetta al Responsabile Iniziale del trattamento assicurare che il sub-Responsabile del trattamento presenti garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per l'adozione di misure tecniche ed organizzative appropriate di modo che il trattamento risponda ai principi e alle esigenze del Regolamento UE. In caso di mancato adempimento da parte del sub-Responsabile del trattamento degli obblighi in materia di protezione dei dati, il Responsabile Iniziale del trattamento è interamente responsabile nei confronti del Titolare del trattamento di tali inadempimenti; l'Amministrazione potrà in qualsiasi momento verificare le garanzie e le misure tecniche ed organizzative del sub-Responsabile, tramite audit e ispezioni anche avvalendosi di soggetti terzi. Nel caso in cui tali garanzie risultassero insussistenti o inadeguate l'Amministrazione potrà risolvere il contratto con il Responsabile iniziale.

Nel caso in cui all'esito delle verifiche, ispezioni e audit le misure di sicurezza dovessero risultare inapplicate o inadeguate rispetto al rischio del trattamento o, comunque, inadeguate ad assicurare l'applicazione del Regolamento, l'Amministrazione applicherà al Fornitore/Responsabile Iniziale del trattamento la penale di cui all'Accordo Quadro e diffiderà lo stesso a far adottare al sub-Responsabile del trattamento tutte le misure più opportune entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a tale diffida, la Committente potrà risolvere il contratto con il Responsabile iniziale ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno;

Il Responsabile del trattamento manleverà e terrà indenne il Titolare da ogni perdita, contestazione, responsabilità, spese sostenute nonché dei costi subiti (anche in termini di danno reputazionale) in relazione anche ad una sola violazione della normativa in materia di Trattamento dei Dati Personali e/o del Contratto (inclusi gli Allegati) comunque derivata



- dalla condotta (attiva e/o omissiva) sua e/o dei suoi agenti e/o sub-fornitori.
- 22.9 Il Responsabile del trattamento deve assistere il Titolare del trattamento al fine di dare seguito alle richieste per l'esercizio dei diritti degli interessati ai sensi degli artt. da 15 a 23 del Regolamento UE; qualora gli interessati esercitino tale diritto presso il Responsabile del trattamento, quest'ultimo è tenuto ad inoltrare tempestivamente, e comunque nel più breve tempo possibile, le istanze al Titolare del Trattamento, supportando quest'ultimo al fine di fornire adeguato riscontro agli interessati nei termini prescritti.
- 22.10 Il Responsabile del trattamento informa tempestivamente e, in ogni caso senza ingiustificato ritardo dall'avvenuta conoscenza, il Titolare di ogni violazione di dati personali (cd. data breach); tale notifica è accompagnata da ogni documentazione utile, ai sensi degli artt. 33 e 34 del Regolamento UE, per permettere al Titolare del trattamento, ove ritenuto necessario, di notificare questa violazione all'Autorità Garante per la protezione dei dati personali, entro il termine di 72 ore da quanto il Titolare ne viene a conoscenza; nel caso in cui il Titolare debba fornire informazioni aggiuntive all'Autorità di controllo, il Responsabile del trattamento supporterà il Titolare nella misura in cui le informazioni richieste e/o necessarie per l'Autorità di controllo siano esclusivamente in possesso del Responsabile del trattamento e/o di suoi sub-Responsabili.
- 22.11 Il Responsabile del trattamento deve avvisare tempestivamente e senza ingiustificato ritardo il Titolare in caso di ispezioni, di richiesta di informazioni e di documentazione da parte dell'Autorità Garante per la protezione dei dati personali; inoltre, deve assistere il Titolare nel caso di richieste formulate dall'Autorità Garante in merito al trattamento dei dati personali effettuate in ragione del presente contratto;
- 22.12 Il Responsabile del trattamento deve mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al Regolamento UE, oltre a contribuire e consentire al Titolare - anche tramite soggetti terzi dal medesimo autorizzati, dandogli piena collaborazione - verifiche periodiche o circa l'adeguatezza e l'efficacia delle misure di sicurezza adottate ed il pieno e scrupoloso rispetto delle norme in materia di trattamento dei dati personali. A tal fine, il Titolare informa preventivamente il Responsabile del trattamento con un preavviso minimo di tre giorni lavorativi, fatta comunque salva la possibilità di effettuare controlli a campione senza preavviso; nel caso in cui all'esito di tali verifiche periodiche, ispezioni e audit le misure di sicurezza dovessero risultare inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del Regolamento, l'Amministrazione applicherà la penale di cui all'Accordo Quadro e diffiderà il Fornitore ad adottare tutte le misure più opportune entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a seguito della diffida, la Committente potrà risolvere il contratto ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.
- 22.13 Il Responsabile del trattamento deve comunicare al Titolare del trattamento il nome ed i dati del proprio "Responsabile della protezione dei dati", qualora, in ragione dell'attività svolta, ne abbia designato uno conformemente all'articolo 37 del Regolamento UE; il Responsabile della protezione dei dati personali del Fornitore/Responsabile collabora e si tiene in costante contatto con il Responsabile della protezione dei dati del Titolare.
- 22.14 Al termine della prestazione dei servizi oggetto del contratto, il Responsabile su richiesta del Titolare, si impegna a: i) restituire al Titolare del trattamento i supporti rimovibili



- eventualmente utilizzati su cui sono memorizzati i dati; ii) distruggere tutte le informazioni registrate su supporto fisso, documentando per iscritto l'adempimento di tale operazione.
- 22.15 Il Responsabile si impegna a attuare quanto previsto dal provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 e s.m.i. recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratori di sistema".
- 22.16 In via generale, il Responsabile del trattamento si impegna ad operare adottando tutte le misure tecniche e organizzative, le attività di formazione, informazione e aggiornamento ragionevolmente necessarie per garantire che i Dati Personali trattati in esecuzione del presente contratto, siano precisi, corretti e aggiornati nel corso della durata del trattamento - anche qualora il trattamento consista nella mera custodia o attività di controllo dei dati - eseguito dal Responsabile, o da un sub-Responsabile.
- 22.17 Su richiesta del Titolare, il Responsabile si impegna ad adottare, nel corso dell'esecuzione del Contratto, ulteriori garanzie quali l'applicazione di un codice di condotta approvato o di un meccanismo di certificazione approvato di cui agli articoli 40 e 42 del Regolamento UE, quando verranno emanati. L'Amministrazione potrà in ogni momento verificare l'adozione di tali ulteriori garanzie.
- 22.18 Il Responsabile non può trasferire i dati personali verso un paese terzo o un'organizzazione internazionale salvo che non abbia preventivamente ottenuto l'autorizzazione scritta da parte del Titolare.
- 22.19 Sarà obbligo del Titolare del trattamento vigilare durante tutta la durata del trattamento, sul rispetto degli obblighi previsti dalle presenti istruzioni e dal Regolamento UE sulla protezione dei dati da parte del Responsabile del trattamento, nonché a supervisionare l'attività di trattamento dei dati personali effettuando audit, ispezioni e verifiche periodiche sull'attività posta in essere dal Responsabile del trattamento.
- 22.20 Nel caso in cui il Fornitore agisca in modo difforme o contrario alle legittime istruzioni del Titolare oppure adotti misure di sicurezza inadeguate rispetto al rischio del trattamento risponde del danno causato agli "interessati". In tal caso, l'Amministrazione potrà risolvere il contratto ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.
- 22.21 Durante l'esecuzione del Contratto, nell'eventualità di qualsivoglia modifica della normativa in materia di Trattamento dei Dati Personali che generi nuovi requisiti (ivi incluse nuove misure di natura fisica, logica, tecnica, organizzativa, in materia di sicurezza o trattamento dei dati personali), il Responsabile del trattamento si impegna a collaborare - nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse - con il Titolare affinché siano sviluppate, adottate e implementate misure correttive di adeguamento ai nuovi requisiti.

Letto, approvato e sottoscritto

Roma, lì \_\_\_\_\_

\_\_\_\_\_  
(per l'Amministrazione)

\_\_\_\_\_  
(per il Fornitore)

Classificazione: Consip Public

Procedura aperta per la conclusione di un Accordo Quadro avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni - Lotto 2 - ID SIGEF 2296

Allegato F - Schema di Contratto Esecutivo



Ai sensi e per gli effetti dell'art. 1341 c.c. il Fornitore dichiara di aver letto con attenzione e di approvare specificatamente le pattuizioni contenute negli articoli seguenti: Art. 1 Definizioni, Art. 3 Oggetto del Contratto esecutivo, Art. 4 Efficacia e durata, Art. 5 Gestione del Contratto esecutivo, Art. 6 Presa in carico e trasferimento del Know How, Art. 7 Locali messi a disposizione dell'Amministrazione contraente, Art. 8 Verifiche di conformità, Art. 9 Penali, Art. 10 Corrispettivi, Art. 11 Fatturazione e pagamenti, Art. 12 Garanzia dell'esatto adempimento, *<ove previsto>*, Art. 13 Subappalto, *<ove previsto>*, Art. 14 Condizioni e Test richiesti dal CVCN, Art. 15 Risoluzione e Recesso, Art. 16 Forza Maggiore, Art. 17 Responsabilità civile *<ove prevista>* e polizza assicurativa, Art. 18 Trasparenza dei prezzi, Art. 19 Oneri fiscali e spese contrattuali, Art. 20 Tracciabilità dei flussi finanziari Art. 21 Foro competente, Art. 22 Trattamento dei dati personali

Letto, approvato e sottoscritto

Roma, lì

---

(per il Fornitore)



**ALLEGATO G – DISPOSIZIONI PER LA GOVERNANCE**



**consip**



**DIPARTIMENTO**  
PER LA TRASFORMAZIONE  
DIGITALE



**AGID**

Agenzia per l'Italia Digitale

## **Piano Strategico ICT**

### **Governance delle Gare Strategiche**

**Disposizioni per la governance**

**Categorizzazione, Indicatori di digitalizzazione**



consip



DIPARTIMENTO  
PER LA TRASFORMAZIONE  
DIGITALE



AGID

Agenzia per l'Italia Digitale

## Sommario

1.	PREMESSA .....	4
2.	DEFINIZIONI .....	4
3.	PERIMETRO.....	5
4.	MONITORAGGIO DELL'APPLICAZIONE DEL PIANO TRIENNALE.....	6
4.1	Elementi caratterizzanti .....	6
5.	PRINCIPI GUIDA.....	7
6.	CATEGORIZZAZIONE DEI CONTRATTI ESECUTIVI RISPETTO AL PIANO TRIENNALE 2020-2022 .....	8
6.1	Categorizzazione di I livello dei contratti esecutivi .....	8
6.2	Categorizzazione di II livello dei contratti esecutivi.....	11
6.3	Contratti ad alta rilevanza.....	15
7.	MONITORAGGIO DEI RISULTATI DI DIGITALIZZAZIONE .....	17
7.1	Indicatori Generali di digitalizzazione .....	17
7.2	Indicatori Specifici di digitalizzazione.....	27
7.3	Indicatori II livello per contratti ad alta rilevanza .....	37



consip



DIPARTIMENTO  
PER LA TRASFORMAZIONE  
DIGITALE



AGID

Agenzia per l'Italia Digitale

## Indice delle tabelle

Tabella 1 - Obiettivi del Piano Triennale .....	9
Tabella 2 - Categorizzazione di I livello (Gare Strategiche pubblicate 2019-2020) .....	10
Tabella 3 - Categorizzazione generale di II livello.....	12
Tabella 4 - Categorizzazione di II livello (Gare Strategiche pubblicate 2019-2020) .....	14
Tabella 5 - Criteri per l'identificazione dei Contratti Esecutivi ad <i>alta rilevanza</i> .....	16
Tabella 6 - Indicatori Generali di digitalizzazione .....	18
Tabella 7 - Indicatori Generali quantitativi.....	21
Tabella 8 - Indicatori Generali qualitativi .....	24
Tabella 9 - Indicatori generali di riuso .....	26
Tabella 10 - Indicatori Specifici Digital Transformation.....	29
Tabella 11 - Indicatori Specifici Public cloud IaaS e PaaS .....	31
Tabella 12 - Indicatori Specifici Servizi Applicativi in ottica cloud .....	32
Tabella 13 - Indicatori specifici Data Management .....	34
Tabella 14 - Indicatore di progresso .....	35
Tabella 15 - Indicatori specifici II livello Servizi Applicativi in ottica cloud.....	39
Tabella 16 - Indicatori specifici II Data Management .....	40



## 1. PREMESSA

Il presente documento illustra gli elementi essenziali della governance delle Gare Strategiche del Piano ICT 2019<sup>1</sup> elaborato da AgID e Consip.

Le misure indicate hanno l'obiettivo di abilitare il monitoraggio di coerenza dei Contratti Esecutivi che saranno sottoscritti dalle Amministrazioni a partire dagli Accordi Quadro stipulati da Consip con gli aggiudicatari di ciascuna Gara Strategica.

## 2. DEFINIZIONI

- **Categorizzazione:** inquadramento o classificazione rispetto al Piano Triennale per l'Informatica nella Pubblica Amministrazione, ed. 2019-2021 e successive
- **Organismi di coordinamento e controllo:** differenziati in Organismi tecnici e Organismo strategico, sono le Strutture deputate alla governance dell'esecuzione dei Contratti derivanti dalle Gare Strategiche.
- **Organismo tecnico di coordinamento e controllo:** struttura organizzativa, nominata per ciascuna Gara, altresì definito **Comitato Tecnico**. È composto da rappresentanti istituzionali – individuati in AgID e Consip, anche integrati con altri soggetti terzi da questi individuati e da rappresentanti del Fornitore/dei Fornitori aggiudicatari della specifica procedura di gara (Gara Strategica).
- **Organismo Strategico di coordinamento e controllo:** struttura organizzativa unica, altresì definita **Comitato Strategico**, per la governance di tutte le gare strategiche del Piano ICT 2019, composta da rappresentanti di AgID, Consip e dal Dipartimento per la Trasformazione digitale, individuati dai medesimi soggetti.
- **Gestione del transiente:** attività, progetti e contratti finalizzati al mantenimento del funzionamento *as is* dei sistemi e delle applicazioni dell'Amministrazione.
- **Contratti ad alta rilevanza:** Contratti Esecutivi caratterizzati da elementi di volume, valore, tecnologia, rilevanza nazionale, di particolare interesse ai fini del coordinamento e controllo operato dal Comitato Strategico.
- **Dati di governance:** principi, categorizzazione, indicatori generali e specifici di digitalizzazione.
- **Valore ex ante:** si intende la misura rilevata per l'indicatore di riferimento prima dell'avvio delle attività contrattualizzate dall'Amministrazione con il Fornitore e finalizzate al raggiungimento dell'obiettivo del Contratto Esecutivo.
- **Valore ex post:** si intende la misura rilevata per l'indicatore di riferimento a valle del completamento delle attività contrattualizzate dall'Amministrazione con il Fornitore e finalizzate al raggiungimento dell'obiettivo del Contratto Esecutivo.
- **Intervento:** insieme di più attività svolte mediante i servizi di un contratto Esecutivo; l'intervento è identificato da un obiettivo che l'Amministrazione intende raggiungere con lo svolgimento delle attività che lo compongono.

---

<sup>1</sup> Comprensivo delle sue evoluzioni.



### 3. PERIMETRO

Le misure e le modalità descritte nel presente documento si applicano alle seguenti Gare Strategiche:

- Digital Transformation (ID 2069),
- Public Cloud IaaS e PaaS (ID 2213),
- Servizi Applicativi in ottica cloud (ID 2212),
- Data Management (ID 2102),
- Fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-apt ed erogazione di servizi connessi per le Pubbliche Amministrazioni (ID 2367),
- Gara a procedura aperta per l'affidamento di un Accordo Quadro per la fornitura di prodotti per la gestione degli eventi di sicurezza e degli accessi, la protezione dei canali email, web e dati ed erogazione di servizi connessi per le Pubbliche Amministrazioni (ID 2174),
- Servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni (ID 2296)<sup>2</sup>,
- Sanità digitale 1 - sistemi informativi clinico assistenziali (ID 2202),
- Sanità digitale 2 - sistemi informativi sanitari e servizi al cittadino (ID 2365),
- Sanità digitale 3 - sistemi informativi gestionali (ID 2366),
- Public Cloud SaaS<sup>3</sup>.

---

<sup>2</sup> ID 2296 è bandita ai sensi dell'art. 4, comma 3-quater, del D.L. n. 95/2012, come convertito con modificazioni dalla Legge n. 135/2012, che ha stabilito che, per la realizzazione di quanto previsto dall'art. 20 del D.L. n. 83/2012, Consip S.p.A. svolge altresì le attività di centrale di committenza relativamente "ai contratti-quadro ai sensi dell'articolo 1, comma 192, della legge 30 dicembre 2004, n. 311". Per la merceologia trattata è considerata al pari delle gare strategiche.

<sup>3</sup> Tutte le gare che saranno definite.





#### 4. MONITORAGGIO DELL'APPLICAZIONE DEL PIANO TRIENNALE

Al fine di monitorare il recepimento dei principi e delle indicazioni del Piano Triennale per l'Informatica nella Pubblica Amministrazione (più avanti anche solo Piano Triennale), in particolare rispetto alla sua edizione 2020-2022, si aggiorna come di seguito descritto la categorizzazione dei contratti esecutivi che saranno stipulati sugli Accordi Quadro relativi alle Gare Strategiche.

- Riferimento alla documentazione di gara: CT generale delle 4 gare strategiche pubblicate 2019-2020 – Categorizzazione
- Applicabilità: ciascun contratto esecutivo, sia esso derivante da ordine diretto o da rilancio competitivo, non si applica ai contratti esecutivi riferiti alla *gestione del transiente*<sup>4</sup>
- Soggetto impattato: l'Amministrazione che stipula un contratto esecutivo
- Modalità di censimento dell'informazione:
  - a) Per i contratti scaturenti da ordine diretto, nel caso di gare che prevedono il Piano dei Fabbisogni, le informazioni richieste saranno esplicitate nel Piano dei Fabbisogni e/o nei suoi allegati, in ogni caso secondo standard e modalità messi a disposizione da Consip S.p.A. alla stipula dell'AQ;
  - b) Per i contratti scaturenti da ordine diretto, nel caso di gare che non prevedono il Piano dei Fabbisogni, le informazioni richieste saranno esplicitate in allegati alla documentazione contrattuale predisposti secondo standard messi a disposizione da Consip S.p.A. alla stipula dell'AQ;
  - c) Per i contratti scaturenti da rilancio competitivo, le informazioni dovranno essere esplicitate in allegati alla documentazione contrattuale predisposti secondo standard messi a disposizione da Consip S.p.A., alla stipula dell'AQ;
- Vincoli temporali per la raccolta delle informazioni: in quanto informazioni allegate alla documentazione contrattuale, entro la stipula del contratto esecutivo in caso di ordine diretto, e in allegato alla documentazione di Appalto Specifico in caso di rilancio competitivo.
- Regole di applicazione/calcolo: negli standard forniti da Consip, in via propedeutica rispetto all'esplicitazione della categorizzazione, dei principi e degli indicatori, l'Amministrazione dovrà indicare se il Contratto Esecutivo è riferito alla *gestione del transiente*.

##### 4.1 ELEMENTI CARATTERIZZANTI

Il monitoraggio riguarda:

- i **principi guida** che l'Amministrazione prevede di seguire attraverso la realizzazione delle attività oggetto l'ordine/AS;
- la **categorizzazione**, cioè la mappatura, del Contratto Esecutivo, stipulato dall'Amministrazione, rispetto agli ambiti (layer) del Piano Triennale per l'informatica nella Pubblica Amministrazione 2020-2022.

---

<sup>4</sup> Come definita nel par. 2 - Definizioni



## 5. PRINCIPI GUIDA

L'Amministrazione, in maniera facoltativa, potrà indicare i principi guida che prevede di seguire attraverso l'ordine/AS, selezionando uno o più dei seguenti, in base alla applicabilità allo specifico AQ di riferimento:

- *Digital & mobile first* (digitale e mobile come prima opzione): le Pubbliche Amministrazioni devono realizzare servizi primariamente digitali;
- *digital identity only* (accesso esclusivo mediante identità digitale): le Pubbliche Amministrazioni devono adottare in via esclusiva sistemi di identità digitale definiti dalla normativa assicurando almeno l'accesso tramite SPID;
- *cloud first* (cloud come prima opzione): le Pubbliche Amministrazioni, in fase di definizione di un nuovo progetto e di sviluppo di nuovi servizi, adottano primariamente il paradigma cloud, tenendo conto della necessità di prevenire il rischio di lock-in;
- servizi inclusivi e accessibili: le Pubbliche Amministrazioni devono progettare servizi pubblici digitali che siano inclusivi e che vengano incontro alle diverse esigenze delle persone e dei singoli territori;
- dati pubblici un bene comune: il patrimonio informativo della pubblica amministrazione è un bene fondamentale per lo sviluppo del Paese e deve essere valorizzato e reso disponibile ai cittadini e alle imprese, in forma aperta e interoperabile;
- interoperabile by design: i servizi pubblici devono essere progettati in modo da funzionare in modalità integrata e senza interruzioni in tutto il mercato unico esponendo le opportune API;
- sicurezza e *privacy by design*: i servizi digitali devono essere progettati ed erogati in modo sicuro e garantire la protezione dei dati personali;
- *user-centric, data driven* e *agile*: le Amministrazioni sviluppano i servizi digitali, prevedendo modalità agili di miglioramento continuo, partendo dall'esperienza dell'utente e basandosi sulla continua misurazione di prestazioni e utilizzo.
- *once only*: le Pubbliche Amministrazioni devono evitare di chiedere ai cittadini e alle imprese informazioni già fornite;
- transfrontaliero *by design* (concepito come transfrontaliero): le Pubbliche Amministrazioni devono rendere disponibili a livello transfrontaliero i servizi pubblici digitali rilevanti;
- *open source*: le Pubbliche Amministrazioni devono prediligere l'utilizzo di software con codice sorgente aperto e, nel caso di software sviluppato per loro conto, deve essere reso disponibile il codice sorgente.



## 6. CATEGORIZZAZIONE DEI CONTRATTI ESECUTIVI RISPETTO AL PIANO TRIENNALE 2020-2022

Per ciascun Contratto Esecutivo, ad esclusione di quanto soggetto a segreto di Stato e delle classifiche di segretezza, l'Amministrazione avrà l'**obbligo**<sup>5</sup> di indicare gli ambiti (o *layer*) – cosiddetti di I livello - e i relativi obiettivi del Piano Triennale che essa prevede di mappare mediante le attività che saranno svolte con il Contratto esecutivo in oggetto.

Per ciascuno degli ambiti scelti, l'Amministrazione potrà selezionare, tra quelli presenti, uno o più obiettivi.

La categorizzazione prevede:

- un inquadramento di I livello, che si applica a tutti i contratti esecutivi;
- un inquadramento di II livello, che si applica solo ai contratti esecutivi definiti ad "alta rilevanza" secondo i criteri più appresso definiti per ciascuna Gara Strategica.

### 6.1 CATEGORIZZAZIONE DI I LIVELLO DEI CONTRATTI ESECUTIVI

La seguente tabella sintetizza la Categorizzazione e gli obiettivi associati:

Ambito I livello (layer)	Obiettivi Piano Triennale
Servizi	<ul style="list-style-type: none"> <li>• Servizi al cittadino</li> <li>• Servizi a imprese e professionisti</li> <li>• Servizi interni alla propria PA</li> <li>• Servizi verso altre PA</li> </ul>
Dati	<ul style="list-style-type: none"> <li>• Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese</li> <li>• Aumentare la qualità dei dati e dei metadati</li> <li>• Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati</li> </ul>
Piattaforme	<ul style="list-style-type: none"> <li>• Favorire l'evoluzione delle piattaforme esistenti per migliorare i servizi offerti a cittadini ed imprese semplificando l'azione amministrativa</li> <li>• Aumentare il grado di adozione ed utilizzo delle piattaforme abilitanti esistenti da parte delle PA</li> <li>• Incrementare e razionalizzare il numero di piattaforme per le amministrazioni al fine di semplificare i servizi ai cittadini</li> </ul>

<sup>5</sup> Come da CT generale delle Gare strategiche pubblicate 2019-2020.



Ambito I livello (layer)	Obiettivi Piano Triennale
Infrastrutture	<ul style="list-style-type: none"> <li>• Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni locali favorendone l'aggregazione e la migrazione sul territorio (Riduzione Data Center sul territorio)</li> <li>• Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni centrali favorendone l'aggregazione e la migrazione su infrastrutture sicure ed affidabili (Migrazione infrastrutture interne verso il paradigma cloud)</li> <li>• Migliorare la fruizione dei servizi digitali per cittadini ed imprese tramite il potenziamento della connettività per le PA</li> </ul>
Interoperabilità	<ul style="list-style-type: none"> <li>• Favorire l'applicazione della Linea guida sul Modello di Interoperabilità da parte degli erogatori di API</li> <li>• Adottare API conformi al Modello di Interoperabilità</li> </ul>
Sicurezza Informatica	<ul style="list-style-type: none"> <li>• Aumentare la consapevolezza del rischio cyber (Cyber Security Awareness) nelle PA</li> <li>• Aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione</li> </ul>

Tabella 1 - Obiettivi del Piano Triennale

Rispetto alla categorizzazione completa di cui alla Tabella 1 - Obiettivi del Piano Triennale, per ciascuna Gara Strategica si individuano nei seguenti paragrafi i layer applicabili.

**6.1.1 CATEGORIZZAZIONE DEI CONTRATTI ESECUTIVI PER LE GARE STRATEGICHE PUBBLICATE 2019-2020**

Gara Strategica	Ambito I livello applicabile
Digital Transformation	<ul style="list-style-type: none"> <li>• Servizi</li> <li>• Dati</li> <li>• Piattaforme</li> <li>• Infrastrutture</li> <li>• Interoperabilità</li> <li>• Sicurezza Informatica</li> </ul>
Public Cloud IaaS e PaaS	<ul style="list-style-type: none"> <li>• Servizi</li> <li>• Infrastrutture</li> <li>• Dati</li> </ul>
Servizi applicativi in ottica cloud	<ul style="list-style-type: none"> <li>• Servizi</li> <li>• Piattaforme</li> <li>• Interoperabilità</li> </ul>
Data Management	<ul style="list-style-type: none"> <li>• Dati</li> </ul>

Tabella 2 - Categorizzazione di I livello (Gare Strategiche pubblicate 2019-2020)

**6.1.2 CATEGORIZZAZIONE DEI CONTRATTI ESECUTIVI PER LE GARE STRATEGICHE IN PREDISPOSIZIONE**

Per le seguenti iniziative:

- Fornitura di prodotti per la sicurezza perimetrale, protezione degli end point e anti-apt ed erogazione di servizi connessi per le Pubbliche Amministrazioni (ID 2367),
- Fornitura di prodotti per la gestione degli eventi di sicurezza e degli accessi, la protezione dei canali email, web e dati ed erogazione di servizi connessi per le Pubbliche Amministrazioni (ID 2174),
- Fornitura di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni – (ID 2296),

Si applicano almeno gli ambiti di I livello *Sicurezza Informatica* e *Infrastrutture*.

- Per le Gare Strategiche SaaS varrà tutto quanto specificato per il solo Lotto 1 della Public Cloud.
- Per le Gare Strategiche di Sanità Digitale, la categorizzazione sarà definita in documentazione di gara, compatibilmente con i tempi già previsti per la pubblicazione dei bandi, o comunque nel corso delle attività propedeutiche alla stipula dei relativi AQ.



## 6.2 CATEGORIZZAZIONE DI II LIVELLO DEI CONTRATTI ESECUTIVI

Per i contratti ad *alta rilevanza* le Amministrazioni contraenti dettagliano i dati forniti secondo quanto indicato nel seguito.

Le informazioni relative alla categorizzazione sono fornite con le stesse modalità e tempistiche previste per la categorizzazione di I livello (cfr. par. 6.1)

In particolare, le Amministrazioni provvedono a:

1. Raffinare le indicazioni sugli ambiti di I livello (layer), indicando gli ambiti di II livello mediante una selezione, anche multipla, dalla categorizzazione riportata nella seguente tabella:

Ambito I (layer)	Ambito II livello
Servizi	<ul style="list-style-type: none"> <li>• Servizi al cittadino</li> <li>• Servizi a imprese e professionisti</li> <li>• Servizi interni alla propria PA</li> <li>• Servizi verso altre PA</li> </ul>
Dati	<ul style="list-style-type: none"> <li>• Agricoltura, pesca, silvicoltura e prodotti alimentari</li> <li>• Economia e finanze</li> <li>• Istruzione, cultura e sport</li> <li>• Energia</li> <li>• Ambiente</li> <li>• Governo e Settore pubblico</li> <li>• Salute</li> <li>• Tematiche internazionali</li> <li>• Giustizia e sicurezza pubblica</li> <li>• Regioni e città</li> <li>• Popolazione e società</li> <li>• Scienza e tecnologia</li> <li>• Trasporti</li> </ul>
Piattaforme	<ul style="list-style-type: none"> <li>• Sanità digitale (FSE e CUP)</li> <li>• Identità Digitale;</li> <li>• Pagamenti digitali;</li> <li>• App IO;</li> <li>• ANPR;</li> <li>• NoiPA;</li> <li>• INAD;</li> <li>• Musei;</li> <li>• Siope+</li> </ul>
Infrastrutture	<ul style="list-style-type: none"> <li>• Data Center e Cloud</li> <li>• Connettività</li> </ul>
Interoperabilità	<ul style="list-style-type: none"> <li>• Agricoltura, pesca, silvicoltura e prodotti alimentari</li> <li>• Economia e finanze</li> <li>• Istruzione, cultura e sport</li> <li>• Energia</li> <li>• Ambiente</li> </ul>





Ambito I (layer)	Ambito II livello
	<ul style="list-style-type: none"> <li>• Governo e Settore pubblico</li> <li>• Salute</li> <li>• Tematiche internazionali</li> <li>• Giustizia e sicurezza pubblica</li> <li>• Regioni e città</li> <li>• Popolazione e società</li> <li>• Scienza e tecnologia</li> <li>• Trasporti</li> </ul>
Sicurezza informatica	<ul style="list-style-type: none"> <li>• Portali istituzionali e CMS</li> <li>• Sensibilizzazione del rischio cyber</li> </ul>

Tabella 3 - Categorizzazione generale di II livello

**6.2.1 CATEGORIZZAZIONE DI II LIVELLO DEI CONTRATTI ESECUTIVI PER LE GARE STRATEGICHE PUBBLICATE 2019-2020**

Nell'applicazione di quanto sopra descritto, l'amministrazione terrà conto degli ambiti applicabili come già descritti per la categorizzazione di I livello e riportati nella seguente tabella:

Gara strategica	Ambito I livello applicabile	Ambito II livello applicabile
Digital Transformation	Tutti	Tutti
Public Cloud IaaS e PaaS	<ul style="list-style-type: none"> <li>Servizi</li> </ul>	<ul style="list-style-type: none"> <li>Servizi al cittadino</li> <li>Servizi a imprese e professionisti</li> <li>Servizi interni alla propria PA</li> <li>Servizi verso altre PA</li> </ul>
	<ul style="list-style-type: none"> <li>Infrastrutture</li> </ul>	<ul style="list-style-type: none"> <li>Agricoltura, pesca, silvicoltura e prodotti alimentari</li> <li>Economia e finanze</li> <li>Istruzione, cultura e sport</li> <li>Energia</li> <li>Ambiente</li> <li>Governo e Settore pubblico</li> <li>Salute</li> <li>Tematiche internazionali</li> <li>Giustizia e sicurezza pubblica</li> <li>Regioni e città</li> <li>Popolazione e società</li> <li>Scienza e tecnologia</li> <li>Trasporti</li> </ul>
	<ul style="list-style-type: none"> <li>Dati</li> </ul>	<ul style="list-style-type: none"> <li>Data Center e Cloud</li> <li>Connettività</li> </ul>
Servizi applicativi in ottica cloud	<ul style="list-style-type: none"> <li>Servizi</li> </ul>	<ul style="list-style-type: none"> <li>Servizi al cittadino</li> <li>Servizi a imprese e professionisti</li> <li>Servizi interni alla propria PA</li> <li>Servizi verso altre PA</li> </ul>
	<ul style="list-style-type: none"> <li>Piattaforme</li> </ul>	<ul style="list-style-type: none"> <li>Sanità digitale (FSE e CUP)</li> <li>Identità Digitale</li> <li>Pagamenti digitali</li> <li>App IO</li> <li>ANPR</li> <li>NoiPA</li> <li>INAD</li> <li>Musei</li> </ul>

		<ul style="list-style-type: none"><li>• Siope+</li></ul>
	<ul style="list-style-type: none"><li>• Interoperabilità</li></ul>	<ul style="list-style-type: none"><li>• Agricoltura, pesca, silvicoltura e prodotti alimentari</li><li>• Economia e finanze</li><li>• Istruzione, cultura e sport</li><li>• Energia</li><li>• Ambiente</li><li>• Governo e Settore pubblico</li><li>• Salute</li><li>• Tematiche internazionali</li><li>• Giustizia e sicurezza pubblica</li><li>• Regioni e città</li><li>• Popolazione e società</li><li>• Scienza e tecnologia</li><li>• Trasporti</li></ul>
Data Management	<ul style="list-style-type: none"><li>• Dati</li></ul>	<ul style="list-style-type: none"><li>• Agricoltura, pesca, silvicoltura e prodotti alimentari</li><li>• Economia e finanze</li><li>• Istruzione, cultura e sport</li><li>• Energia</li><li>• Ambiente</li><li>• Governo e Settore pubblico</li><li>• Salute</li><li>• Tematiche internazionali</li><li>• Giustizia e sicurezza pubblica</li><li>• Regioni e città</li><li>• Popolazione e società</li><li>• Scienza e tecnologia</li><li>• Trasporti</li></ul>

Tabella 4 - Categorizzazione di II livello (Gare Strategiche pubblicate 2019-2020)

#### 6.2.2 CATEGORIZZAZIONE DI II LIVELLO DEI CONTRATTI ESECUTIVI PER LE GARE STRATEGICHE IN PREDISPOSIZIONE

Fermo restando l'obbligo per le Amministrazioni di indicare gli ambiti di I livello e i relativi obiettivi del Piano Triennale, per le iniziative di Sicurezza Informatica ci si riserva la possibilità di definire prima della stipula dell'Accordo Quadro eventuali ambiti di II Livello più specifici per una mappatura più mirata degli interventi in ambito Cyber Security da parte delle PA.

Per le altre iniziative la categorizzazione di II livello sarà definita congiuntamente ad AgID e al Dipartimento in tempo utile per la stipula dei relativi contratti di AQ.



### 6.3 CONTRATTI AD ALTA RILEVANZA

Nel seguente paragrafo si riportano, per ciascuna delle Gare Strategiche pubblicate nel periodo 2019-2020 (Digital Transformation, Public Cloud IaaS e PaaS, Servizi applicativi in ottica cloud e Data Management), le caratteristiche di rilevanza individuate in funzione delle peculiarità dei servizi e degli obiettivi della gara di riferimento.

Si precisa che, in ogni caso, il Comitato Strategico potrà includere nel novero dei contratti ad alta rilevanza anche altre tipologie, quali ad esempio i contratti inerenti l'interoperabilità, le piattaforme abilitanti e in generale, rilevanti ai fini del processo di avanzamento della trasformazione digitale e dell'adozione del modello Cloud nella PA.

Per le Gare strategiche in predisposizione:

- Fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-apt ed erogazione di servizi connessi per le Pubbliche Amministrazioni (ID 2367);
- Gara a procedura aperta per l'affidamento di un Accordo Quadro per la fornitura di prodotti per la gestione degli eventi di sicurezza e degli accessi, la protezione dei canali email, web e dati ed erogazione di servizi connessi per le Pubbliche Amministrazioni (ID 2174);
- Servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni (ID 2296);

e per le Gare Strategiche attinenti alla Sanità digitale, ci si riserva la possibilità di definire prima della stipula degli Accordi Quadro i criteri per l'identificazione dei Contratti Esecutivi *ad alta rilevanza*.

Gara strategica	Lotto	criteri	indicatori aggiuntivi
Digital Transformation	Lotto 1 Lotto 2	<ul style="list-style-type: none"> <li>• Lotto 1: Contratti Esecutivi di importo &gt; € 450.000,00 i.e.</li> <li>• Lotto 2: Contratti Esecutivi di importo &gt; € 400.000,00 i.e.</li> </ul>	<ul style="list-style-type: none"> <li>• Non si prevedono indicatori aggiuntivi per i contratti esecutivi ad alta rilevanza.</li> <li>• Per i Lotti dal 3 al 9, trattandosi di lotti di servizi complementari a quelli previsti per Lotto 1 e Lotto 2, non si prevedono soglie specifiche.</li> </ul>
Public Cloud IaaS e PaaS		<ul style="list-style-type: none"> <li>• Lotto 1: Contratti Esecutivi che includono più di 3 categorie di servizi del configuratore; oppure Contratti Esecutivi di importo &gt; € 500.000,00 i.e.</li> <li>• Lotti 2-11: contratti esecutivi &gt; € 250.000,00 i.e.</li> </ul>	Nessun indicatore aggiuntivo



Gara strategica	Lotto	criteri	indicatori aggiuntivi
Servizi applicativi in ottica <i>cloud</i>		<ul style="list-style-type: none"> <li>Lotti 1 e 2: Contratti Esecutivi di importo &gt; € 10.000.000,00 i.e.</li> <li>Lotti 3,4,5: n.a.</li> <li>Lotti 6,7,8,9: n.a.</li> </ul>	Previsti (cfr. 7.3.3)
Data Management		<ul style="list-style-type: none"> <li>Lotti 1,2,3: Contratti Esecutivi di importo &gt; € 1.000.000,00 i.e.</li> </ul>	Previsti (cfr 7.3.4)

**Tabella 5 - Criteri per l'identificazione dei Contratti Esecutivi ad *alta rilevanza***

Per quanto riguarda le Gare Strategiche in predisposizione, eventuali criteri per identificare Contratti ad alta rilevanza saranno definiti entro la stipula, congiuntamente ad AgID e Dipartimento.



## 7. MONITORAGGIO DEI RISULTATI DI DIGITALIZZAZIONE

Al fine di abilitare un puntuale monitoraggio dei risultati ottenuti dalle Amministrazioni in termini di digitalizzazione mediante l'utilizzo degli Accordi Quadro relativi alle Gare Strategiche sono stati previsti, in documentazione di gara, ed articolati nel presente documento indicatori così classificati:

- **Indicatori Generali di digitalizzazione**, che mappano il macro-obiettivo dell'intervento rispetto ai principali obiettivi strategici del Piano Triennale;
- **Indicatori Specifici di digitalizzazione**, che definiscono, sulla base delle specificità della Gara Strategica, le misure di digitalizzazione applicabili allo specifico contratto esecutivo, in funzione dei prodotti/servizi acquisiti.

Gli indicatori sono utilizzati per il monitoraggio dei contratti e del raggiungimento dei relativi obiettivi, così come dettagliati nel Piano dei Fabbisogni e nel Piano Operativo.

Ciascuna Amministrazione, all'atto di definizione del Piano dei Fabbisogni o altra specifica documentazione contrattuale laddove il Piano dei Fabbisogni non sia previsto, individuerà almeno un Indicatore Generale per il quale fornirà, agli Organismi di coordinamento e controllo e/o ai soggetti da questi indicati, le misure di riferimento ex ante ed ex post rispetto al contratto esecutivo.

### 7.1 INDICATORI GENERALI DI DIGITALIZZAZIONE

- Riferimento alla documentazione di gara: CT generale delle 4 gare strategiche pubblicate 2019-2020 – Categorizzazione
- Applicabilità: ciascun contratto esecutivo, sia esso derivante da ordine diretto o da rilancio competitivo, ad esclusione di quelli relativi alla *gestione del transiente o che includono unicamente servizi di gestione e/o di supporto*, ad esclusione di quanto soggetto a segreto di Stato e delle classifiche di segretezza
- Soggetto impattato: l'Amministrazione che stipula un contratto esecutivo
- Modalità di raccolta dell'informazione:
  - a) Per i contratti scaturenti da ordine diretto, nel caso di gare che prevedono il Piano dei Fabbisogni, le informazioni richieste saranno esplicitate nel Piano dei Fabbisogni e/o nei suoi allegati;
  - b) Per i contratti scaturenti da ordine diretto, nel caso di gare che non prevedono il Piano dei Fabbisogni, le informazioni richieste saranno esplicitate in allegati alla documentazione contrattuale predisposti secondo standard messi a disposizione da Consip S.p.A. alla stipula dell'AQ;
  - c) Per i contratti scaturenti da rilancio competitivo, le informazioni dovranno essere esplicitate in allegati alla documentazione di gara relativa all'AS, predisposti secondo standard messi a disposizione da Consip S.p.A.
- Vincoli temporali per la scelta degli indicatori: in quanto informazioni allegate alla documentazione contrattuale, entro la stipula del contratto esecutivo in caso di ordine diretto, e contestualmente alla pubblicazione dell'Appalto Specifico, in allegato alla documentazione in caso di rilancio competitivo; in alternativa, per le gare in ambito Sicurezza, in caso di ordine diretto senza Piano dei Fabbisogni, entro la data di emissione del Piano di Lavoro Generale.





La misura *ex post* sarà fornita, al completamento delle attività contrattuali, con un aggiornamento degli allegati utilizzati per fornire i dati di governance, con particolare riferimento agli indicatori di digitalizzazione, e tracciato nel portale del Fornitore che ha eseguito l'intervento oggetto di misura, nei tempi previsti per l'aggiornamento dei dati sul Portale stesso.

- Regole di applicazione/calcolo: in via propedeutica rispetto all'esplicitazione della categorizzazione, dei principi e degli indicatori, l'Amministrazione dovrà indicare, negli standard forniti da Consip, se il Contratto Esecutivo è riferito alla *gestione del transiente*.

Gli indicatori generali di digitalizzazione, validi per tutte le Gare Strategiche, sono i seguenti:

Indicatori quantitativi	Indicatori qualitativi	Indicatori di collaborazione e riuso
Riduzione % della spesa per l'erogazione del servizio	Obiettivi CAD raggiunti con l'intervento	Riuso di processi per erogazione servizi
Riduzione % dei tempi di erogazione del servizio	Integrazione con infrastrutture immateriali	Riuso soluzioni tecniche
Numero servizi aggiuntivi offerti all'utenza interna, esterna (cittadini), esterna (imprese), altre PA	Integrazione con Basi Dati di interesse nazionale	Collaborazione con altre Amministrazioni (progetto in co-working, realizzato anche mediante contratti esecutivi diversi per Amministrazione)

**Tabella 6 - Indicatori Generali di digitalizzazione**

Per le gare di Sicurezza<sup>6</sup> non è prevista la scelta degli indicatori sopra riportati: i servizi erogati dalle gare infatti, non consentono di costruire logicamente una correlazione tra il servizio acquistato dall'Amministrazione e il contenuto degli indicatori generali.

Nelle seguenti tabelle si riportano le modalità di misurazione degli indicatori generali.

Si precisa che per tutti gli indicatori generali di digitalizzazione:

1. L'oggetto di riferimento è sempre il Contratto Esecutivo;
2. Nel caso in cui con uno stesso Contratto Esecutivo l'Amministrazione voglia realizzare uno o più interventi progettuali, potrà
  - Scegliere l'indicatore con riferimento all'intervento più rilevante in termini di effort/spesa per la realizzazione dello stesso,

<sup>6</sup> Fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-apt ed erogazione di servizi connessi per le Pubbliche Amministrazioni (ID 2367); Gara a procedura aperta per l'affidamento di un Accordo Quadro per la fornitura di prodotti per la gestione degli eventi di sicurezza e degli accessi, la protezione dei canali email, web e dati ed erogazione di servizi connessi per le Pubbliche Amministrazioni (ID 2174); Servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni (ID 2296)



- Scegliere più indicatori riferendone ciascuno ad uno degli interventi la cui realizzazione è prevista con l'acquisizione dei servizi del Contratto Esecutivo.

L'Amministrazione dovrà quindi specificare, secondo gli standard messi a disposizione da Consip, le informazioni relative alla scelta sopra formulata e successivamente, in fase di raccolta del *valore ex post*, specificare, nel caso di più interventi, a quale intervento il valore si riferisce.

Indicatori quantitativi	ID	Modalità di misura	Rilevazione dell'indicatore
Riduzione % della spesa per l'erogazione del servizio	IQT1	<p>Il riferimento è al <b>servizio digitale erogato dall'Amministrazione</b> verso la sua utenza.</p> <p>L'indicatore misura la <u>variazione della spesa</u>, sostenuta dall'Amministrazione e intesa come <b>costo stimato per l'erogazione del servizio digitale, per unità di servizio digitale erogato all'utenza</b>.</p> <p>La variazione è espressa in % e prende in considerazione:</p> <ul style="list-style-type: none"> <li>• Il costo attuale sostenuto dall'Amministrazione per l'erogazione di una unità di servizio digitale, <u>calcolato prima dell'avvio delle attività del Contratto Esecutivo di pertinenza</u><sup>7</sup></li> <li>• Il costo aggiornato sostenuto dall'Amministrazione per l'erogazione di una unità di servizio digitale, <u>calcolato a valle del completamento delle attività del Contratto Esecutivo di pertinenza</u>.</li> </ul> <p>Nello stimare il costo l'Amministrazione terrà conto delle componenti hw, sw, di risorse professionali per la gestione interna e idealmente il TCO, qualora disponibile.</p>	<ul style="list-style-type: none"> <li>• Valore <i>ex ante</i> rispetto all'intervento<sup>8</sup>, in termini di <b>stima della riduzione del costo per l'erogazione del servizio digitale, per unità di servizio digitale erogato</b>;</li> <li>• Valore <i>ex post</i>, al completamento dell'intervento<sup>9</sup>, in termini di <b>misura effettiva della riduzione del costo per l'erogazione del servizio digitale, per unità di servizio digitale erogato</b></li> </ul>

<sup>7</sup> Nel caso in cui le attività riguardino uno o più interventi inclusi nel Contratto Esecutivo, l'Amministrazione terrà conto solo di quelli pertinenti al raggiungimento dell'obiettivo e quindi coerenti con l'indicatore scelto.

<sup>8</sup> o agli interventi di pertinenza come esplicitato nelle modalità di misura.

<sup>9</sup> Vedi nota precedente.

Indicatori quantitativi	ID	Modalità di misura	Rilevazione dell'indicatore
Riduzione % dei tempi di erogazione del servizio	IQT2	<p>Il riferimento è al <b>servizio digitale erogato dall'Amministrazione</b> verso la sua utenza.</p> <p>L'indicatore misura la <u>variazione del tempo di erogazione del servizio digitale</u> da parte dell'Amministrazione e inteso come <b>il tempo intercorrente tra la "richiesta", da parte dell'utente del servizio digitale verso l'Amministrazione, e la disponibilità dell'oggetto del servizio</b> all'utente stesso.</p> <p>La variazione è espressa in % e prende in considerazione:</p> <ul style="list-style-type: none"> <li>• Il tempo attuale intercorrente tra la richiesta da parte dell'utente dell'Amministrazione mediante il servizio digitale, per l'erogazione di una unità di servizio digitale, <u>calcolato prima dell'avvio delle attività del Contratto Esecutivo di pertinenza<sup>10</sup></u></li> <li>• Il tempo aggiornato intercorrente tra la richiesta da parte dell'utente dell'Amministrazione mediante il servizio digitale, per l'erogazione di una unità di servizio digitale, <u>calcolato a valle del completamento delle attività del Contratto Esecutivo di pertinenza<sup>11</sup></u></li> </ul>	<ul style="list-style-type: none"> <li>• Valore <i>ex ante</i> rispetto all'intervento<sup>12</sup>, in termini di <b>stima della riduzione del tempo di erogazione del servizio digitale, per unità di servizio digitale erogato</b>;</li> <li>• Valore <i>ex post</i>, al completamento dell'intervento<sup>13</sup>, in termini di <b>misura effettiva della riduzione del tempo di erogazione del servizio digitale, per unità di servizio digitale erogato</b>.</li> </ul>

<sup>10</sup> Nel caso in cui le attività riguardino uno o più interventi inclusi nel Contratto Esecutivo, l'Amministrazione terrà conto solo di quelli pertinenti al raggiungimento dell'obiettivo e quindi coerenti con l'indicatore scelto.

<sup>11</sup> Vedi nota precedente.

<sup>12</sup> o agli interventi di pertinenza come esplicitato nelle modalità di misura.

<sup>13</sup> Vedi nota precedente.

Indicatori quantitativi	ID	Modalità di misura	Rilevazione dell'indicatore
Numero servizi aggiuntivi offerti all'utenza interna, esterna (cittadini), esterna (imprese), altre PA	IQT3	Quantità di <b>nuovi servizi digitali che l'Amministrazione mette a disposizione della propria utenza</b> , utilizzando le risorse messe a disposizione dal Contratto Esecutivo; La quantità è espressa in termini assoluti, per ciascuna tipologia di utente.	<ul style="list-style-type: none"> <li>• Valore <i>ex ante</i> rispetto all'intervento<sup>14</sup>, in termini di <b>numero di nuovi servizi digitali che l'Amministrazione intende realizzare e mettere a disposizione della propria utenza mediante il Contratto Esecutivo</b>;</li> <li>• Valore <i>ex post</i>, al completamento dell'intervento<sup>15</sup>, in termini di numero effettivo di nuovi servizi digitali <b>che l'Amministrazione ha messo a disposizione della propria utenza mediante il Contratto Esecutivo</b>.</li> </ul>

**Tabella 7 - Indicatori Generali quantitativi**

<sup>14</sup> o agli interventi di pertinenza come esplicitato nelle modalità di misura.

<sup>15</sup> Vedi nota precedente.

Indicatori qualitativi	ID	Modalità di misura	Rilevazione dell'indicatore
Obiettivi CAD raggiunti con l'intervento <sup>16</sup>	IQL1	Selezione ed indicazione <sup>17</sup> di uno o più obiettivi CAD <sup>18</sup> : <ul style="list-style-type: none"> <li>• Diritto all'uso delle tecnologie</li> <li>• Partecipazione al procedimento amministrativo informatico</li> <li>• Effettuazione dei pagamenti con modalità informatiche</li> <li>• Utilizzo della posta elettronica certificata</li> <li>• Qualità dei servizi resi e soddisfazione dell'utenza</li> <li>• Alfabetizzazione informatica dei cittadini</li> <li>• Partecipazione democratica elettronica</li> <li>• Sportelli per le attività produttive</li> <li>• Registro informatico degli adempimenti amministrativi per le imprese</li> </ul>	<ul style="list-style-type: none"> <li>• Valore <i>ex ante</i> rispetto all'intervento<sup>19</sup>, in termini di <b>indicazione degli obiettivi CAD che l'amministrazione intende raggiungere con le attività previste in Contratto Esecutivo;</b></li> <li>• Valore <i>ex post</i> rispetto all'intervento<sup>20</sup>, in termini di <b>indicazione degli obiettivi CAD effettivamente raggiunti dall'Amministrazione con le attività previste in Contratto Esecutivo.</b></li> </ul>

<sup>16</sup> Anche in questo caso, l'Amministrazione può far riferimento alle attività previste dall'intero contratto esecutivo, oppure ad una sua parte (uno o più interventi).

<sup>17</sup> Mediante gli strumenti e/o gli standard messi a disposizione da Consip.

<sup>18</sup> Gli obiettivi sono quelli riportati nella **"Sezione II. Diritti dei cittadini e delle imprese" del "Capo I Principi generali del CAD**. La selezione sarà fatta sullo standard fornito da Consip.

<sup>19</sup> o agli interventi di pertinenza come esplicitato nelle modalità di misura.

<sup>20</sup> o agli interventi di pertinenza come esplicitato nelle modalità di misura.

Indicatori qualitativi	ID	Modalità di misura	Rilevazione dell'indicatore
Integrazione con infrastrutture immateriali	IQL2	Selezione ed indicazione <sup>21</sup> di una o più infrastrutture immateriali di cui al Piano Triennale.	<ul style="list-style-type: none"><li>• Valore <i>ex ante</i> rispetto all'intervento<sup>22</sup>, in termini di <b>indicazione delle infrastrutture immateriali che l'Amministrazione intende integrare con le attività previste in Contratto Esecutivo;</b></li><li>• Valore <i>ex post</i> rispetto all'intervento<sup>23</sup>, in termini di <b>indicazione delle infrastrutture effettivamente integrate dall'Amministrazione con le attività previste in Contratto Esecutivo.</b></li></ul>

---

<sup>21</sup> Mediante gli strumenti e/o gli standard messi a disposizione da Consip.

<sup>22</sup> o agli interventi di pertinenza come esplicitato nelle modalità di misura.

<sup>23</sup> o agli interventi di pertinenza come esplicitato nelle modalità di misura.





Indicatori qualitativi	ID	Modalità di misura	Rilevazione dell'indicatore
Integrazione con Basi Dati di interesse nazionale	IQL3	Selezione ed indicazione <sup>24</sup> di una o più Basi Dati di interesse nazionale.	<ul style="list-style-type: none"> <li>Valore <i>ex ante</i> rispetto all'intervento<sup>25</sup>, in termini di <b>indicazione delle Basi Dati di interesse nazionale che l'Amministrazione intende integrare con le attività previste in Contratto Esecutivo;</b></li> <li>Valore <i>ex post</i> rispetto all'intervento<sup>26</sup>, in termini di <b>indicazione delle Basi Dati di interesse nazionale effettivamente integrate dall'Amministrazione con le attività previste in Contratto Esecutivo.</b></li> </ul>

Tabella 8 - Indicatori Generali qualitativi

<sup>24</sup> Mediante gli strumenti e/o gli standard messi a disposizione da Consip.

<sup>25</sup> o agli interventi di pertinenza come esplicitato nelle modalità di misura.

<sup>26</sup> o agli interventi di pertinenza come esplicitato nelle modalità di misura.

Indicatori di collaborazione e riuso	ID	Modalità di misura	Rilevazione dell'indicatore
Riuso di processi per erogazione servizi	ICR1	Indicazione dei processi (e laddove applicabile), del loro numero e delle Amministrazioni delle quali si riutilizza il processo	<ul style="list-style-type: none"> <li>Valore <i>ex ante</i>: <b>elencazione dei processi</b> e delle Amministrazioni di riferimento del riuso dei processi <b>che l'Amministrazione intende riusare</b> nel Contratto Esecutivo;</li> <li>Valore <i>ex post</i>: elencazione dei <b>processi effettivamente riutati dall'Amministrazione</b> nelle attività del Contratto Esecutivo.</li> </ul>
Riuso soluzioni tecniche	ICR2	Indicazione delle soluzioni tecniche riutilizzate e della/delle Amministrazione/i della/e quale/i si riutilizzano le soluzioni	<ul style="list-style-type: none"> <li>Valore <i>ex ante</i>: <b>elencazione delle soluzioni tecniche</b> e delle Amministrazioni di riferimento <b>che l'Amministrazione intende riusare</b> nel Contratto Esecutivo;</li> <li>Valore <i>ex post</i>: elencazione <b>delle soluzioni tecniche effettivamente riusate dall'Amministrazione</b> nelle attività del Contratto Esecutivo.</li> </ul>



Indicatori di collaborazione e riuso	ID	Modalità di misura	Rilevazione dell'indicatore
Collaborazione con altre Amministrazioni (progetto in co-working)	ICR3	Indicazione delle Amministrazioni coinvolte nel progetto <sup>27</sup> in coworking	<ul style="list-style-type: none"> <li>Valore <i>ex ante</i>: <b>elencazione delle Amministrazioni coinvolte nella realizzazione del progetto in coworking con le quali l'Amministrazione collaborerà utilizzando le risorse del Contratto Esecutivo;</b></li> <li>Valore <i>ex ante</i>: <b>elencazione delle Amministrazioni con le quali l'Amministrazione ha effettivamente collaborato.</b></li> </ul>

Tabella 9 - Indicatori generali di riuso

Eventuali ulteriori elementi di dettaglio per la rilevazione degli indicatori generali saranno forniti alla stipula/attivazione dell'Accordo Quadro, o comunque secondo le modalità e i tempi concordati dall'Organismo di Coordinamento e Controllo finalizzato alla direzione strategica e/o secondo quanto più precisamente definito in corso d'opera all'atto della stipula/attivazione degli Accordi Quadro delle Gare Strategiche Digital Transformation, Public Cloud IaaS e PaaS, Servizi Applicativi in ottica cloud e Data Management.

Si precisa che, fatte salve le previsioni della documentazione di gara

- I valori *ex ante* dovranno essere forniti secondo gli standard messi a disposizione da Consip e comunque allegati alla documentazione contrattuale del Contratto Esecutivo, nel caso di Ordini, e allegati alla documentazione di AS nel caso di rilancio competitivo;
- I valori *ex post* dovranno essere forniti dall'Amministrazione, con il supporto del Fornitore, entro la chiusura formale del Contratto Esecutivo e resi disponibili sul Portale del Fornitore nei tempi previsti per l'aggiornamento periodico.

<sup>27</sup> Per progetto si intende in questo caso un insieme complesso di attività realizzato in coworking da più Amministrazioni, ciascuna mediante uno o più contratti esecutivi volti a realizzare uno o più interventi funzionali alla realizzazione del progetto in coworking.



## 7.2 INDICATORI SPECIFICI DI DIGITALIZZAZIONE

Sono individuati sulla base delle caratteristiche specifiche dei servizi, individuati nella documentazione di gara o – laddove previsto – demandati alle valutazioni degli Organismi di coordinamento e controllo. Laddove non presenti in documentazione di gara, le modalità di rilevazione e le relative tempistiche saranno oggetto di specifiche appendici contrattuali per ciascuna gara.

### 7.2.1 INDICATORI SPECIFICI DI DIGITALIZZAZIONE PER LA GARA STRATEGICA DIGITAL TRANSFORMATION

Lotto/servizio	ID	Indicatori specifici
L1.S1 Disegno strategia digitale	DTL1S1.1	<ul style="list-style-type: none"> <li>• disponibilità piano economico-finanziario (collegato all'implementazione della strategia)</li> </ul>
	DTL1S1.2	<ul style="list-style-type: none"> <li>• numero di linee del Piano Triennale indirizzate nella strategia rispetto al totale delle linee applicabili</li> </ul>
	DTL1S1.2	<ul style="list-style-type: none"> <li>• numero di obiettivi pianificati a 3 anni sul totale obiettivi pianificati nella strategia</li> </ul>
L1.S2 Disegno del Piano Strategico ICT	DTL1S2.1	<ul style="list-style-type: none"> <li>• disponibilità piano economico-finanziario (collegato all'implementazione del Piano Strategico ICT)</li> </ul>
	DTL1S2.2	<ul style="list-style-type: none"> <li>• numero di linee del Piano Triennale indirizzate nella strategia rispetto al totale delle linee applicabili</li> </ul>
	DTL1S2.3	<ul style="list-style-type: none"> <li>• numero di obiettivi pianificati a 3 anni sul totale obiettivi pianificati nella strategia</li> </ul>
	DTL1S2.4	<ul style="list-style-type: none"> <li>• efficientamento atteso della spesa ICT</li> </ul>
L1.S3 <sup>28</sup> Disegno della mappa dei servizi digitali dell'Amministrazione	DTL1S3.1	<ul style="list-style-type: none"> <li>• % servizi digitali mappati rispetto al totale servizi digitali erogati dall'Amministrazione</li> </ul>
	DTL1S3.2	<ul style="list-style-type: none"> <li>• Numero di nuovi servizi digitali mappati rispetto al totale dei servizi digitali erogati dall'Amministrazione</li> </ul>
L2.S1	DTL2S1.1	<ul style="list-style-type: none"> <li>• % servizi digitali con modello di erogazione disegnato/censito rispetto al totale servizi digitali erogati dall'Amministrazione</li> </ul>

<sup>28</sup> In valutazione la fattibilità di inserimento di un indicatore volto a misurare il totale dei servizi erogati dall'Amministrazione



Lotto/servizio	ID	Indicatori specifici
Disegno del modello di erogazione del servizio digitale	DTL2S1.2	<ul style="list-style-type: none"> <li>% servizi digitali con nuovo modello di erogazione rispetto al totale servizi digitali erogati dall'Amministrazione</li> </ul>
L2.S2 Disegno del processo digitale sotteso all'erogazione del servizio digitale	DTL2S2.1	<ul style="list-style-type: none"> <li>numero di processi digitali sottesi all'erogazione di servizi disegnati ex novo</li> </ul>
	DTL2S2.2	<ul style="list-style-type: none"> <li>numero di processi digitali reingegnerizzati</li> </ul>
	DTL2S2.3	<ul style="list-style-type: none"> <li>numero di servizi digitalizzati end to end per ogni milestone di pianificazione</li> </ul>
L2.S3 Supporto specialistico per le attività propedeutiche all'implementazione del servizio digitale	DTL2S3.1	<u>per Supporto alla definizione di interventi di riorganizzazione e Supporto al disegno del processo sotteso al servizio digitale:</u> <ul style="list-style-type: none"> <li>Rapporto tra valore (spesa) per supporto e valore dell'intervento di disegno dei processi digitali per il quale si richiede supporto</li> </ul>
	DTL2S3.2	<u>per Supporto alla definizione di interventi di riorganizzazione e Supporto al disegno del processo sotteso al servizio digitale:</u> <ul style="list-style-type: none"> <li>Rapporto tra numero di processi digitali e numero di giornate di supporto acquistate</li> </ul>
	DTL2S3.3	<u>per Supporto alla valutazione degli strumenti di acquisizione</u> <ul style="list-style-type: none"> <li>Rapporto tra valore (spesa) per supporto e valore dell'intervento di trasformazione per il quale l'Amministrazione richiede supporto</li> </ul>
	DTL2S3.4	<u>per Supporto alla valutazione degli strumenti di acquisizione</u> <ul style="list-style-type: none"> <li>Rapporto tra Numero di strumenti di acquisizione valutati mediante l'attività di supporto e numero di giornate di supporto acquistate</li> </ul>
L3.S1, L4.S1, L5.S1 Progettazione della Transizione Digitale	-	Non previsti
L3.S2, L4.S2, L5.S2 Affiancamento alla Transizione Digitale	DTL3S2.1 DTL4S2.1 DTL5S2.1	<ul style="list-style-type: none"> <li>% di utenti formati sul totale utenti previsti</li> </ul>
	DTL3S2.2 DTL4S2.2 DTL5S2.2	<ul style="list-style-type: none"> <li>livello di adozione del contenuto di trasformazione digitale.</li> </ul>



Lotto/servizio	ID	Indicatori specifici
L6.S1, L7.S1, L8.S1 PMO di programmi di digitalizzazione	-	Non previsti
L6.S2, L7.S2, L8.S2 PMO di progetti cross ambito	-	Non previsti
L6.S3, L7.S3, L8.S3 Supporto alla gestione dei progetti e dei programmi collegati alla Digital Transformation	-	Non previsti
L9.S1 Supporto alla Governance	-	Non previsti

Tabella 10 - Indicatori Specifici Digital Transformation



## 7.2.2 INDICATORI SPECIFICI DI DIGITALIZZAZIONE PER LA GARA STRATEGICA PUBLIC CLOUD IAAS E PAAS

Lotto/Servizio	ID	Indicatori
<b>LOTTO 1</b> <b>SERVIZI IAAS:</b> <ul style="list-style-type: none"> <li>• Categoria Compute;</li> <li>• Categoria Storage;</li> <li>• Categoria Network;</li> <li>• Categoria Security;</li> <li>• Categoria Monitoring.</li> </ul>	PCL1I.1	<ul style="list-style-type: none"> <li>• Layer INFRASTRUTTURE: <ul style="list-style-type: none"> <li>✓ Riduzione % di RAM disponibile su data center</li> </ul> </li> </ul>
	PCL1I.2	<ul style="list-style-type: none"> <li>• Layer INFRASTRUTTURE: <ul style="list-style-type: none"> <li>✓ Riduzione % di CPU disponibile su data center</li> </ul> </li> </ul>
	PCL1I.3	<ul style="list-style-type: none"> <li>• Layer INFRASTRUTTURE: <ul style="list-style-type: none"> <li>✓ Riduzione % di Storage disponibile su data center</li> </ul> </li> </ul>
	PCL1I.4	<ul style="list-style-type: none"> <li>• Layer SERVIZI: <ul style="list-style-type: none"> <li>✓ Numero di servizi cloud qualificati acquistati</li> </ul> </li> </ul>
<b>LOTTO 1</b> <b>SERVIZI PAAS:</b> <ul style="list-style-type: none"> <li>○ Categoria Containers;</li> <li>○ Categoria Database;</li> <li>○ Categoria Developer Tools;</li> <li>○ Categoria Application Platform.</li> </ul>	PCL1P.1	<ul style="list-style-type: none"> <li>• Layer INFRASTRUTTURE: <ul style="list-style-type: none"> <li>✓ Riduzione % di RAM disponibile su data center</li> </ul> </li> </ul>
	PCL1P.2	<ul style="list-style-type: none"> <li>• Layer INFRASTRUTTURE: <ul style="list-style-type: none"> <li>✓ Riduzione % di CPU disponibile su data center</li> </ul> </li> </ul>
	PCL1P.3	<ul style="list-style-type: none"> <li>• Layer INFRASTRUTTURE: <ul style="list-style-type: none"> <li>✓ Riduzione % di Storage disponibile su data center</li> </ul> </li> </ul>
	PCL1P.4	<ul style="list-style-type: none"> <li>• Layer SERVIZI: <ul style="list-style-type: none"> <li>✓ Numero di servizi cloud qualificati acquistati</li> </ul> </li> </ul>
<b>LOTTE 2-6</b> <ul style="list-style-type: none"> <li>• ASSESSMENT (S1)</li> <li>• STRATEGIA DI MIGRAZIONE (S2)</li> <li>• CHECK DEI RISULTATI (S5)</li> </ul>	PCL2.1 PCL3.1 PCL4.1 PCL5.1 PCL6.1	<ul style="list-style-type: none"> <li>• Layer SERVIZI: <ul style="list-style-type: none"> <li>✓ Numero di servizi digitali esistenti erogati in modalità on-premise oggetto di assessment</li> </ul> </li> </ul>
	PCL2.2 PCL3.2 PCL4.2 PCL5.2 PCL6.2	<ul style="list-style-type: none"> <li>• Layer SERVIZI: <ul style="list-style-type: none"> <li>✓ Numero di servizi migrati in cloud</li> </ul> </li> </ul>





Lotto/Servizio	ID	Indicatori
	PCL2.3 PCL3.3 PCL4.3 PCL5.3 PCL6.3	<ul style="list-style-type: none"> <li>Layer SERVIZI:               <ul style="list-style-type: none"> <li>✓ % di servizi migrati in cloud rispetto a quelli esistenti e oggetto di assessment.</li> </ul> </li> </ul>
<b>LOTTE 7-11</b> SERVIZI DI SOLUTION DESIGN E ARCHITECTURE <ul style="list-style-type: none"> <li>Disegno dei workload (M1.1)</li> <li>Implementazione migrazione (M1.2)</li> <li>Trasferimento Dati (M2.2)</li> </ul>	PCL7.1 PCL8.1 PCL9.1 PCL10.1 PCL11.1	<ul style="list-style-type: none"> <li>Layer SERVIZI:               <ul style="list-style-type: none"> <li>✓ Numero di servizi esistenti migrabili in cloud mediante re-host</li> </ul> </li> </ul>
	PCL7.2 PCL8.2 PCL9.2 PCL10.2 PCL11.2	<ul style="list-style-type: none"> <li>Layer SERVIZI:               <ul style="list-style-type: none"> <li>✓ Numero di servizi esistenti migrabili in cloud mediante re-platform</li> </ul> </li> </ul>
	PCL7.3 PCL8.3 PCL9.3 PCL10.3 PCL11.3	<ul style="list-style-type: none"> <li>Layer SERVIZI:               <ul style="list-style-type: none"> <li>✓ Numero di servizi esistenti migrabili in cloud mediante re-purchase</li> </ul> </li> </ul>
	PCL7.4 PCL8.4 PCL9.4 PCL10.4 PCL11.4	<ul style="list-style-type: none"> <li>Layer INFRASTRUTTURE:               <ul style="list-style-type: none"> <li>✓ Riduzione % di RAM/CPU/Storage disponibile post-migrazione mediante re-purchase</li> </ul> </li> </ul>
	PCL7.5 PCL8.5 PCL9.5 PCL10.5 PCL11.5	<ul style="list-style-type: none"> <li>Layer DATI:               <ul style="list-style-type: none"> <li>✓ Numero di basi di dati migrati.</li> </ul> </li> </ul>

Tabella 11 - Indicatori Specifici Public cloud IaaS e PaaS



### 7.2.3 INDICATORI SPECIFICI DI DIGITALIZZAZIONE PER LA GARA STRATEGICA SERVIZI APPLICATIVI IN OTTICA CLOUD

Gli indicatori di seguito riportati rappresentano la “specializzazione” di secondo livello degli indicatori applicata ai Contratti Esecutivi identificati come “ad alta rilevanza” secondo i parametri riportati per la Gara strategica Servizi applicativi in ottica cloud nel presente documento.

Modalità e periodicità di misura si intendono dettagliati nei documenti per la stipula dei contratti esecutivi.

Lotto/Servizio	ID	Indicatori
Tutti (tranne PMO)	SAC.1	1. Miglioramento servizi digitalizzati: nr servizi al cittadino-impresa digitalizzati/nr di servizi che richiedono interazione con il cittadino/imprese
	SAC.2	2. Miglioramento dell'esperienza del cittadino/impresa dei sistemi applicativi realizzati/modificati
	SAC.3	3. Standardizzazione strumenti per la generazione e diffusione dei servizi digitali: % componenti di navigazione e interfaccia standard ed usabili /totale componenti
	SAC.4	4. Riutilizzabilità – co-working soluzioni applicative realizzate e/o adottate: nr di progetti in riuso o co-working /nr totale dei progetti di digitalizzazione ove è applicabile il riuso o co-working
	SAC.5	5. Innalzamento livello di interoperabilità: numero di progetti conformi alle linee guida di interoperabilità e nel rispetto del ONCE ONLY principle /Nr progetti realizzati
	SAC.6	6. Potenziamento infrastrutture IT- adozione sistematica del paradigma cloud: nr di progetti conformi al paradigma cloud/totale di progetti realizzati
	SAC.7	7. Utilizzo piattaforme abilitanti: nr di progetti che integrano Piattaforme Abilitanti/nr progetti ove è applicabile un'integrazione con le Piattaforme Abilitanti

**Tabella 12 - Indicatori Specifici Servizi Applicativi in ottica cloud**

**7.2.4 INDICATORI SPECIFICI DI DIGITALIZZAZIONE PER LA GARA STRATEGICA DATA MANAGEMENT**

Servizio	ID	Indicatori
<b>DATA WAREHOUSE E BUSINESS INTELLIGENCE</b> LA.DW.1 - Sviluppo e manutenzione evolutiva di software ad hoc LA.DW.2 - Parametrizzazione e personalizzazione di soluzioni commerciali LA.DW.3 - Gestione applicativa e basi dati LA.DW.4 - Manutenzione correttiva LA.DW.5 - Manutenzione adeguativa LA.DW.6 - Supporto specialistico	DMDWBI.1	<ul style="list-style-type: none"> <li>Produzione/condivisione/messa a disposizione di altre PP.AA. di flussi dati per analisi statistiche/predittive</li> </ul>
	DMDWBI.2	<ul style="list-style-type: none"> <li>Numero di processi digitalizzati che usufruiscono dei dati aggregati prodotti e resi disponibili</li> </ul>
	DMDWBI.3	<ul style="list-style-type: none"> <li>Presenza di flussi di Integrazione/Scambio dati con PDND</li> </ul>
	DMDWBI.4	<ul style="list-style-type: none"> <li>Presenza di flussi di Integrazione/Scambio dati con basi dati di interesse nazionale</li> </ul>
	DMDWBI.5	<ul style="list-style-type: none"> <li>Presenza di flussi di popolamento del Catalogo nazionale dati.gov.it</li> </ul>
	DMDWBI.6	<ul style="list-style-type: none"> <li>Normalizzazione/standardizzazione ontologie e vocabolari in linea con gli obiettivi e le linee d'azione definite nel Piano Triennale AgID</li> </ul>
<b>BIG DATA / ANALYTICS</b> LA.BD.1 - Valutazione e analisi dei dati LA.BD.2 - Acquisizione dati LA.BD.3 - Realizzazione del modello di analisi LA.BD.4 - Conduzione della soluzione di analisi	DMBDA.1	<ul style="list-style-type: none"> <li>Produzione/condivisione/messa a disposizione di altre PP.AA. di flussi dati per analisi statistiche/predittive</li> </ul>
	DMBDA.2	<ul style="list-style-type: none"> <li>Numero di processi digitalizzati che usufruiscono dei dati aggregati prodotti e resi disponibili</li> </ul>
	DMBDA.3	<ul style="list-style-type: none"> <li>Presenza di flussi di Integrazione/Scambio dati con PDND</li> </ul>
	DMBDA.4	<ul style="list-style-type: none"> <li>Presenza di flussi di Integrazione/Scambio dati con basi dati di interesse nazionale</li> </ul>
	DMBDA.5	<ul style="list-style-type: none"> <li>Presenza di flussi di popolamento del Catalogo nazionale dati.gov.it</li> </ul>
	DMBDA.6	<ul style="list-style-type: none"> <li>Normalizzazione/standardizzazione ontologie e vocabolari in linea con gli obiettivi e le linee d'azione definite nel Piano Triennale AgID</li> </ul>
<b>OPEN DATA</b> LA.OD.1 - Analisi dei dati LA.OD.2 - Produzione e metadattazione di dati a livello 3A.OD.3 - Produzione di dati di livello 4 e 5 LA.OD.4 - Pubblicazione dataset	DMOD.1	<ul style="list-style-type: none"> <li>Produzione/condivisione/messa a disposizione di altre PP.AA. di flussi dati per analisi statistiche/predittive</li> </ul>
	DMOD.2	<ul style="list-style-type: none"> <li>Numero di processi digitalizzati che usufruiscono dei dati aggregati prodotti e resi disponibili</li> </ul>
	DMOD.3	<ul style="list-style-type: none"> <li>Open Data: n° dataset pubblicati</li> </ul>



Servizio	ID	Indicatori
LA.OD.5 - Aggiornamento e conservazione dataset	DMOD.4	<ul style="list-style-type: none"> <li>Presenza di flussi di Integrazione/Scambio dati con PDND</li> </ul>
	DMOD.5	<ul style="list-style-type: none"> <li>Presenza di flussi di Integrazione/Scambio dati con basi dati di interesse nazionale</li> </ul>
	DMOD.6	<ul style="list-style-type: none"> <li>Presenza di flussi di popolamento del Catalogo nazionale dati.gov.it</li> </ul>
	DMOD.7	<ul style="list-style-type: none"> <li>Normalizzazione/standardizzazione ontologie e vocabolari in linea con gli obiettivi e le linee d'azione definite nel Piano Triennale AgID</li> </ul>
ARTIFICIAL INTELLIGENCE/MACHINE LEARNING LA.AI.1 - Supporto specialistico	DMAIML.1	<ul style="list-style-type: none"> <li>Produzione/condivisione/messa a disposizione di altre PP.AA. di flussi dati per analisi statistiche/predittive</li> </ul>
	DMAIML.2	<ul style="list-style-type: none"> <li>Numero di processi digitalizzati che usufruiscono dei dati aggregati prodotti e resi disponibili</li> </ul>
	DMAIML.3	<ul style="list-style-type: none"> <li>Presenza di flussi di popolamento del Catalogo nazionale dati.gov.it</li> </ul>
	DMAIML.4	<ul style="list-style-type: none"> <li>Normalizzazione/standardizzazione ontologie e vocabolari in linea con gli obiettivi e le linee d'azione definite nel Piano Triennale AgID</li> </ul>

Tabella 13 - Indicatori specifici Data Management

### 7.2.5 INDICATORI SPECIFICI DI DIGITALIZZAZIONE PER LE GARE DI SICUREZZA

Per le gare di Sicurezza<sup>29</sup> è previsto l'indicatore specifico di digitalizzazione **denominato indicatore di progresso**: per ogni classe di controlli ABSC (Agid Basic Security Control) previsti dalle misure minime di sicurezza AGID (e successive modifiche e integrazioni), sarà calcolato il valore del relativo Indicatore di Progresso (Ip) dell'intervento ottenuto attraverso la realizzazione dell'Ordinativo di Fornitura (acquisto di prodotti e/o servizi previsti nell'Ordinativo), come di seguito riportato:

Denominazione	Indicatore di progresso		
Aspetto da valutare	Grado di mappatura di ciascuna classe di controlli ABSC delle misure minime di sicurezza AGID		
Unità di misura	Numero di Controlli	Fonte dati	Piano dei Fabbisogni o Piano di lavoro Generale
Periodo di riferimento	Momento di Pianificazione dell'intervento	Frequenza di misurazione	Per ogni intervento pianificato
Dati da rilevare	<i>N1: numero di controlli relativi alla specifica classe ABSC soddisfatti attraverso l'intervento</i> <i>NT: numero totale di controlli relativi alla specifica classe previsti dalle misure minime di sicurezza AGID</i>		
Regole di campionamento	Nessuna		
Formula	$Ip = (N_1 - N_0) / N_T$		
Regole di arrotondamento	Nessuna		
Valore di soglia	<i>N0: numero di controlli relativi alla specifica classe soddisfatti prima dell'intervento;</i>		
Applicazione	Amministrazione Contraente		

**Tabella 14 - Indicatore di progresso**

<sup>29</sup> Fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-apt ed erogazione di servizi connessi per le Pubbliche Amministrazioni (ID 2367); Gara a procedura aperta per l'affidamento di un Accordo Quadro per la fornitura di prodotti per la gestione degli eventi di sicurezza e degli accessi, la protezione dei canali email, web e dati ed erogazione di servizi connessi per le Pubbliche Amministrazioni (ID 2174); Servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni (ID 2296)



consip



**DIPARTIMENTO**  
PER LA TRASFORMAZIONE  
DIGITALE



**AGID**

Agenzia per l'Italia Digitale

#### **7.2.6 INDICATORI SPECIFICI DI DIGITALIZZAZIONE PER LE GARE STRATEGICHE IN PREDISPOSIZIONE**

Per tutte le altre gare strategiche in predisposizione e/o pubblicazione gli indicatori saranno definiti in documentazione di gara o comunque entro la stipula, compatibilmente con i tempi di pubblicazione delle stesse.

**7.3 INDICATORI II LIVELLO PER CONTRATTI AD ALTA RILEVANZA****7.3.1 INDICATORI SPECIFICI DI DIGITALIZZAZIONE DI II LIVELLO PER LA GARA STRATEGICA DIGITAL TRANSFORMATION**

Non previsti.

**7.3.2 INDICATORI SPECIFICI DI II LIVELLO PER LA GARA STRATEGICA PUBLIC CLOUD IAAS E PAAS**

Non previsti.

**7.3.3 INDICATORI SPECIFICI DI II LIVELLO PER LA GARA STRATEGICA SERVIZI APPLICATIVI IN OTTICA CLOUD**

IDI	Indicatore di I livello	IDII	Indicatore di II livello
SAC.1	1. Miglioramento servizi digitalizzati: nr servizi al cittadino-impresa digitalizzati/nr di servizi che richiedono interazione con il cittadino/imprese	SAC.1a	• Numero di modelli standard di sviluppo web disponibili tramite Designers Italia che l'Amministrazione intende adottare
		SAC.1b	• Numero di processi operativi/procedure re-ingegnerizzati in ottica di semplificazione mediante la transizione al digitale
		SAC.1c	• Numero di servizi migrati da analogico a digitale
SAC.2	2. Miglioramento dell'esperienza del cittadino/impresa dei sistemi applicativi realizzati/modificati	SAC.2a	• Numero di servizi digitali monitorati tramite Web Analytics Italia (solo per servizi di gestione)
		SAC.2b	• Numero di modelli standard di sviluppo web disponibili tramite Designers Italia che si prevede di adottare
		SAC.2c	• Numero di test di usabilità previsti dalle Linee Guida AGID per il design dei servizi effettuati





IDI	Indicatore di I livello	IDII	Indicatore di II livello
		SAC.2d	<ul style="list-style-type: none"> <li>Numero di siti per i quali è stato rilevato il livello di conformità secondo le Linee guida AgID sull'accessibilità degli strumenti informatici</li> </ul>
SAC.3	3. Standardizzazione strumenti per la generazione e diffusione dei servizi digitali: % componenti di navigazione e interfaccia standard ed usabili /totale componenti	SAC.3a	<ul style="list-style-type: none"> <li>Numero di software open source presente su Developers Italia riutilizzato</li> </ul>
		SAC.3b	<ul style="list-style-type: none"> <li>Numero di software open source pubblicato su Developers Italia</li> </ul>
SAC.4	4. Riusabilità – co-working soluzioni applicative realizzate e/o adottate: nr di progetti in riuso o co-working /nr totale dei progetti di digitalizzazione ove è applicabile il riuso o co-working	SAC.4a	<ul style="list-style-type: none"> <li>Numero di API registrate nel Catalogo</li> </ul>
		SAC.4b	<ul style="list-style-type: none"> <li>Numero di API fruite tramite il Catalogo</li> </ul>
		SAC.4c	<ul style="list-style-type: none"> <li>Numero di servizi digitali per l'interazione erogati dalle PAC ad altre amministrazioni</li> </ul>
		SAC.4d	<ul style="list-style-type: none"> <li>Numero di servizi digitali che utilizzano API registrate nel Catalogo</li> </ul>
SAC.5	5. Innalzamento livello di interoperabilità: numero di progetti conformi alle linee guida di interoperabilità e nel rispetto del ONCE ONLY principle/Nr progetti realizzati	SAC.5a	<ul style="list-style-type: none"> <li>Numero di servizi digitali esistenti on-premise migrati verso servizi cloud qualificati;</li> </ul>
		SAC.5b	<ul style="list-style-type: none"> <li>Numero di nuovi servizi digitali realizzati utilizzando servizi cloud qualificati;</li> </ul>
SAC.7	7. Utilizzo piattaforme abilitanti: nr di progetti che integrano Piattaforme Abilitanti/nr progetti ove è applicabile un'integrazione con le Piattaforme Abilitanti	SAC.7°	<ul style="list-style-type: none"> <li>numero di documenti digitalizzati confluiti nel FSE (referti di medicina di laboratorio e ricette)</li> </ul>
		SAC.7b	<ul style="list-style-type: none"> <li>Percentuale di prenotazioni effettuate online rispetto al totale</li> </ul>
		SAC.7c	<ul style="list-style-type: none"> <li>Numero di servizi offerti da NoiPA utilizzati</li> </ul>
		SAC.7d	<ul style="list-style-type: none"> <li>numero di autenticazioni fatte con SPID e CIE ai servizi online della PA</li> </ul>
		SAC.7e	<ul style="list-style-type: none"> <li>numero di servizi digitali accessibili tramite SPID e CIE</li> </ul>
		SAC.7f	<ul style="list-style-type: none"> <li>numero di servizi digitali integrati con PagoPA</li> </ul>
		SAC.7g	<ul style="list-style-type: none"> <li>numero di servizi digitali integrati con l'App IO</li> </ul>



IDI	Indicatore di I livello	IDII	Indicatore di II livello
		SAC.7h	<ul style="list-style-type: none"> <li>numero di servizi digitali integrati con l'INAD</li> </ul>
		SAC.7i	<ul style="list-style-type: none"> <li>numero di Musei accreditati al Sistema Museale Nazionale.</li> </ul>

Tabella 15 - Indicatori specifici II livello Servizi Applicativi in ottica cloud

**7.3.4 INDICATORI SPECIFICI DI II LIVELLO PER LA GARA STRATEGICA DATA MANAGEMENT**

IDI	Indicatore di I livello	IDII	Indicatore di II livello
DMDWBI.1	Produzione/condivisione/messa a disposizione di altre PP.AA. di flussi dati per analisi statistiche/predittive	DMDWBI.1a	<ul style="list-style-type: none"><li>numero di dataset che adottano un'unica licenza aperta identificata a livello nazionale</li></ul>
		DMDWBI.1b	<ul style="list-style-type: none"><li>numero di basi dati di interesse nazionale che espongono API coerenti con il modello di interoperabilità e con i modelli di riferimento di dati nazionali ed europei</li></ul>
		DMDWBI.1c	<ul style="list-style-type: none"><li>numero di altre PP.AA. coinvolte</li></ul>
DMOD.3	Open Data: n° dataset pubblicati	DMOD.3a	<ul style="list-style-type: none"><li>numero di dataset aperti di tipo dinamico in coerenza con quanto previsto dalla Direttiva (UE) 2019/1024</li></ul>
		DMOD.3b	<ul style="list-style-type: none"><li>numero di dataset resi disponibili attraverso i servizi di dati territoriali di cui alla Direttiva 2007/2/EC (INSPIRE)</li></ul>
		DMOD.3c	<ul style="list-style-type: none"><li>numero di dataset con metadati di qualità conformi agli standard di riferimento europei e dei cataloghi nazionali</li></ul>
		DMOD.3d	<ul style="list-style-type: none"><li>numero di dataset aperti conformi ad un sottoinsieme di caratteristiche di qualità derivate dallo standard ISO/IEC 25012</li></ul>
		DMOD.3e	<ul style="list-style-type: none"><li>numero di dataset che adottano un'unica licenza aperta identificata a livello nazionale</li></ul>

**Tabella 16 - Indicatori specifici II Data Management**

- Fine del documento -

## **ALLEGATO H – REGOLAMENTO DEGLI ORGANISMI DI COORDINAMENTO E CONTROLLO**

# **Piano Strategico ICT Governance delle Gare Strategiche**

**Organismi di coordinamento e controllo**

**Regolamento**

## Sommario

1.	PREMESSA .....	2
2.	DEFINIZIONI .....	2
3.	REGOLAMENTO INTERNO PER IL FUNZIONAMENTO DELL'ORGANISMO TECNICO DI COORDINAMENTO E CONTROLLO .....	4
3.1	Principi generali .....	4
3.2	Compiti e Responsabilità del Comitato Tecnico .....	4
3.3	Individuazione del Presidente - Riunioni del Comitato Tecnico .....	7
3.4	Atti del Comitato Tecnico .....	7
4.	REGOLAMENTO INTERNO PER IL FUNZIONAMENTO DELL'ORGANISMO STRATEGICO DI COORDINAMENTO E CONTROLLO .....	8
4.1	Principi generali .....	8
4.2	Compiti e Responsabilità del Comitato Strategico.....	8
4.3	Riunioni del Comitato Strategico .....	9
4.4	Atti del Comitato Strategico .....	9

## 1. PREMESSA

Il presente documento raccoglie le modalità di funzionamento degli Organismi di coordinamento e controllo deputati alla governance delle Gare afferenti al Piano Strategico ICT 2019<sup>1</sup>, elaborato da AgID con il supporto di Consip e definisce la parte di attività, compiti e responsabilità comuni a tutte le Gare Strategiche, rimandando ai documenti integrativi specifici e/o alle prescrizioni di dettaglio contenute nella documentazione di gara di ciascuna Gara Strategica, per tutti gli aspetti peculiari per i quali non è possibile un funzionamento unitario.

Il regolamento potrà essere rivisto su iniziativa di AgID, Consip o del Dipartimento per la trasformazione digitale.

## 2. DEFINIZIONI

- **Gara Strategica:** iniziativa di acquisizione afferente al Piano Strategico ICT 2019 e sue evoluzioni.

In particolare:

- Digital Transformation (ID 2069),
- Public Cloud IaaS e PaaS (ID 2213),
- Servizi Applicativi in ottica cloud (ID 2212),
- Data Management (ID 2102),
- Fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-apt ed erogazione di servizi connessi per le Pubbliche Amministrazioni (ID 2367),
- Gara a procedura aperta per l'affidamento di un Accordo Quadro per la fornitura di prodotti per la gestione degli eventi di sicurezza e degli accessi, la protezione dei canali email, web e dati ed erogazione di servizi connessi per le Pubbliche Amministrazioni (ID 2174),
- Servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni (ID 2296)<sup>2</sup>,
- Sanità digitale 1 - sistemi informativi clinico assistenziali (ID 2202),
- Sanità digitale 2 - sistemi informativi sanitari e servizi al cittadino (ID 2365),
- Sanità digitale 3 - sistemi informativi gestionali (ID 2366),
- Public Cloud SaaS<sup>3</sup>.

---

<sup>1</sup> Comprensivo delle sue evoluzioni.

<sup>2</sup> ID 2296 è bandita ai sensi dell'art. 4, comma 3-quater, del D.L. n. 95/2012, come convertito con modificazioni dalla Legge n. 135/2012, che ha stabilito che, per la realizzazione di quanto previsto dall'art. 20 del D.L. n. 83/2012, Consip S.p.A. svolge altresì le attività di centrale di committenza relativamente "ai contratti-quadro ai sensi dell'articolo 1, comma 192, della legge 30 dicembre 2004, n. 311". Per la merceologia trattata è considerata al pari delle gare strategiche.

<sup>3</sup> Tutte le gare che saranno definite.



- **Organismi di coordinamento e controllo:** differenziati in Organismo tecnico e Organismo strategico, sono le Strutture deputate alla governance dell'esecuzione dei Contratti derivanti dalle Gare Strategiche.
- **Organismo tecnico di coordinamento e controllo:** struttura organizzativa, nominata per ciascuna Gara, altresì definito **Comitato Tecnico**. È composto da rappresentanti istituzionali di **AgID e Consip**, anche integrati con altri soggetti terzi da questi individuati e da rappresentanti del Fornitore/dei Fornitori aggiudicatari della specifica procedura di gara (Gara Strategica).
- **Organismo Strategico di coordinamento e controllo:** struttura organizzativa unica, altresì definita **Comitato Strategico**, per la governance di tutte le gare strategiche del Piano ICT 2019, composta da rappresentanti istituzionali di AgID, Consip e dal Dipartimento per la Trasformazione digitale, individuati dai medesimi soggetti.
- **Componente pubblica del Comitato Tecnico:** i rappresentanti di AgID e Consip.
- **Fornitore:** operatore economico aggiudicatario della procedura relativa ad una Gara Strategica.

### **3. REGOLAMENTO INTERNO PER IL FUNZIONAMENTO DELL'ORGANISMO TECNICO DI COORDINAMENTO E CONTROLLO**

#### **3.1 PRINCIPI GENERALI**

1. Viene istituito un Comitato Tecnico per ogni Gara Strategica funzionale a tutti i Lotti della medesima Gara;
2. Partecipano al Comitato: AgID, Consip e i fornitori di ciascun Lotto di gara. I rappresentanti degli operatori economici aggiudicatari delle Gare Strategiche hanno diritto a partecipare alle attività del Comitato stesso come di seguito disciplinato;
3. I componenti del Comitato tecnico sono così individuati:
  - ✓ 2 rappresentanti per conto di AgID. Tali rappresentanti possono essere sostituiti mediante delega di AgID da altri rappresentanti (sempre nel numero massimo di 2);
  - ✓ 2 rappresentanti per conto di Consip. Tali rappresentanti possono essere sostituiti mediante delega di Consip da altri rappresentanti (sempre nel numero massimo di 2);
  - ✓ 1 rappresentante per conto dell'/gli aggiudicatario/i di ogni Lotto della Gara Strategica di riferimento. Nel caso in cui il fornitore sia costituito da un RTI, il rappresentante designato dovrà fare capo alla mandataria. Qualora, nell'ambito della documentazione relativa alla specifica Gara Strategica, siano attribuiti al RUAC specifici compiti di interfacciamento con gli organismi di coordinamento e controllo, tale rappresentante dovrà coincidere con il RUAC. In ogni caso, ogni aggiudicatario dovrà indicare anche il nominativo di un supplente (sempre facente capo alla mandataria, in caso di RTI). Il rappresentante (e il supplente) dovranno essere dotati di poteri di rappresentanza dell'azienda;
4. Il Comitato si riunirà almeno quadrimestralmente e comunque, nelle modalità descritte nel presente documento, ogni qualvolta AgID/Consip ne ravvedano la necessità;
5. Il Comitato potrà essere convocato sia relativamente a tematiche riguardanti un singolo Lotto sia per tematiche riguardanti più Lotti; in ogni caso saranno convocati tutti i soggetti dei Lotti coinvolti;
6. Il Comitato potrà coinvolgere qualora necessario una o più Amministrazioni beneficiarie dei contratti derivanti dalla Gara Strategica o soggetti istituzionali competenti su specifiche tematiche.

#### **3.2 COMPITI E RESPONSABILITÀ DEL COMITATO TECNICO**

Si riportano di seguito le attività e le responsabilità in capo al Comitato Tecnico, fermo restando quanto previsto nella documentazione relativa a ciascuna specifica Gara Strategica:

1. monitorare la coerenza dell'impiego dei servizi/forniture messi a disposizione dai diversi Lotti rispetto all'oggetto e al perimetro della Gara Strategica di riferimento e ai vincoli normativi;
2. monitorare il rispetto dei vincoli contrattuali e la qualità della Fornitura;
3. monitorare lo stato di avanzamento dell'Accordo Quadro, in termini di numero di contratti, dimensione degli stessi e massimale complessivo eroso, tramite analisi e approfondimento periodici delle informazioni rese disponibili dal fornitore e prodotti tramite:

- a) formati di office automation fruibili dai componenti del Comitato afferenti a Consip e AgID (esclusi pdf),
- b) link ad aree riservate dei portali di fornitura, con possibilità di download dei contenuti,
- c) altri strumenti messi a disposizione dal Fornitore e/o dai soggetti istituzionali coinvolti nella Governance.

Le informazioni rese disponibili dal Fornitore dovranno contenere almeno il seguente dettaglio minimo:

- a) informazioni tecnico/economiche relative a tutti i contratti esecutivi stipulati con le Amministrazioni; in particolare, dovrà essere disponibile la vista per Amministrazione contenente il dettaglio dei servizi acquistati, con il relativo massimale impegnato ed il consuntivo alla data; tali informazioni dovranno essere rese disponibili mensilmente, entro il 15 del mese successivo al mese di riferimento.
- b) report descrittivi delle iniziative progettuali con periodicità quadrimestrale, resi disponibili almeno 15 giorni lavorativi prima della riunione del Comitato; in particolare per ciascuna Amministrazione si dovrà fornire: una descrizione di massima dell'iniziativa con i relativi obiettivi, eventuale ricorso a soluzioni in riuso (motivando i casi in cui i processi/le soluzioni sviluppate si sono differenziate da pregresse analoghe), eventuale partecipazione di più Amministrazioni al medesimo progetto in modalità di co-working o co-partecipazione finanziaria;

Nel caso in cui la documentazione di gara di ciascuna specifica Gara Strategica preveda informazioni di maggior dettaglio rispetto a quanto sopra descritto, il Fornitore comunque dovrà rendere disponibili al Comitato almeno le viste aggregate che consentano di reperire le informazioni sopra descritte.

Relativamente alla documentazione di cui ai punti precedenti, il Comitato ha facoltà di richiedere al fornitore informazioni aggiuntive/integrative a quelle prodotte.

Si precisa inoltre che la documentazione prodotta dovrà essere resa disponibile anche ai componenti del Comitato Strategico, ove richiesto.

- 4. analizzare i progetti implementati da Amministrazioni diverse nell'ambito degli stessi Accordi Quadro, nei casi specifici, identificati da Consip/AgID o segnalati dalle Amministrazioni, in cui si evidenzino analogie funzionali, tecniche, di obiettivo;
- 5. analizzare le proposte di standardizzazione di processi, modelli, soluzioni, metriche, metodologie di stima dei servizi e, nella sua componente pubblica, valutarne l'adozione, in accordo con il Comitato Strategico;
- 6. valutare le eventuali proposte di evoluzione e/o adeguamento dei servizi o delle forniture da parte del fornitore, laddove espressamente previsto in documentazione di gara e con le procedure definite ad integrazione del presente regolamento;
- 7. monitorare ed eventualmente aggiornare i Livelli di Servizio derivanti da nuovi strumenti di misurazione non disponibili alla data di stipula del contratto e/o derivanti dall'ottimizzazione della rilevazione dei singoli indicatori di qualità;
- 8. monitorare l'andamento degli indicatori di digitalizzazione definiti nella documentazione contrattuale, quelli aggiunti dal Comitato Strategico e quelli aggiuntivi eventualmente offerti dal

- Fornitore, anche attraverso eventuali strumenti messi a disposizione dal fornitore e/o dai soggetti istituzionali coinvolti nella Governance;
9. su richiesta dell'Amministrazione, o per contratti di alta rilevanza segnalati dall'Organismo Strategico di Coordinamento e Controllo, il Comitato Tecnico potrà:
    - a) esaminare specifici Contratti Esecutivi, comprensivi dei relativi allegati (ad esempio Piano dei Fabbisogni, Piano Operativo, etc.);
    - b) dialogare, se necessario, con l'Amministrazione coinvolta e/o il Fornitore di riferimento per l'acquisizione di ulteriori informazioni o l'approfondimento di specifiche tematiche funzionali e/o tecnologiche;
    - c) segnalare all'Amministrazione eventuali criticità/punti di attenzione;
    - d) verificare gli obiettivi raggiunti e il loro eventuale scostamento rispetto al target prefissato;
  10. segnalare al Comitato Strategico progetti con elevata potenzialità di riuso da parte di altre Amministrazioni, anche indicati dalle Amministrazioni o dai fornitori;
  11. richiedere l'intervento del Comitato Strategico (cd. escalation):
    - a) per eventuali criticità rilevate sui contratti esecutivi ad alta rilevanza<sup>4</sup> relativi a progetti speciali e/o di rilevanza nazionale e/o strategici e/o relativi alle piattaforme abilitanti, realizzati o implementati con le gare strategiche;
    - b) in merito ai rapporti con le Amministrazioni e/o i Fornitori;
    - c) in relazione a tutti i punti precedenti.
  12. svolgere qualsiasi altra funzione ad esso attribuita dalla documentazione contrattuale relativa alla specifica Gara Strategica;
  13. valutare e fornire indicazioni ai fornitori, sentito anche il Comitato Strategico, in merito alla necessità di un eventuale adeguamento alle eventuali evoluzioni della normativa tecnica di settore, per quanto compatibile con la documentazione contrattuale relativa alle singole Gare Strategiche.

Per ciascuna Gara Strategica, AgID e Consip, inoltre, valuteranno la predisposizione, all'avvio delle attività dello specifico Comitato Tecnico, di integrazioni al presente regolamento, al fine di regolarne gli aspetti peculiari (es. revisione listini).

Ogni decisione del Comitato si intende validamente assunta se condivisa dai rappresentanti di AgID e Consip. In ogni caso, ogni decisione deve essere previamente comunicata (anche a mezzo di PEC, qualora non presenti alla seduta) a tutti i rappresentanti dei fornitori cui si riferiscono le decisioni assunte (o per Lotti o per merito). I rappresentanti dei fornitori dei Lotti interessati dalla decisione in oggetto hanno altresì diritto di prendere visione degli atti del Comitato, salvo le previsioni di legge in materia, nonché di presentare memorie scritte e documenti, che il Comitato ha l'obbligo di valutare ove siano pertinenti all'oggetto della discussione.

Le decisioni sono assunte nelle forme e nei modi stabiliti da AgID e Consip.

---

<sup>4</sup> Secondo i criteri definiti per ciascuna Gara Strategica

### **3.3 INDIVIDUAZIONE DEL PRESIDENTE - RIUNIONI DEL COMITATO TECNICO**

1. Il ruolo di Presidente del Comitato è ricoperto da un rappresentante di AgID.
2. Le riunioni del Comitato sono convocate dal Presidente o da persona da lui designata, con almeno 5 giorni solari di preavviso, di norma tramite messaggi di posta elettronica certificata (PEC). La nota di convocazione dà indicazione dell'ordine del giorno, che è definito dal Presidente anche sulla base delle proposte, esigenze o richieste espresse da ciascuna parte rappresentata nel Comitato o dalle Amministrazioni. Alla nota di convocazione è allegata eventuale documentazione rilevante ai fini degli argomenti all'ordine del giorno.
3. In funzione degli argomenti trattati, ciascuna parte rappresentata potrà chiamare a partecipare alle riunioni proprio personale di supporto, nel numero massimo di 2 ulteriori persone oltre ai rappresentanti già previsti.
4. Ai fini della validità delle riunioni è necessario che siano presenti almeno i rappresentanti di AgID e Consip e, contestualmente, i fornitori in numero pari alla maggioranza dei fornitori del/i Lotto/i cui si riferisce l'oggetto della riunione.
5. Nel caso in cui non sia raggiunta la validità della seduta, viene riconvocata una nuova seduta che ha validità anche con la sola presenza dei rappresentanti di AgID e Consip.

### **3.4 ATTI DEL COMITATO TECNICO**

1. Gli argomenti discussi nel corso delle riunioni e le decisioni assunte risultano da apposito verbale.
2. Il verbale, redatto dal segretario nominato all'inizio della riunione, è trasmesso in versione preliminare a mezzo posta elettronica a tutti i componenti. La funzione di segretario dovrà essere ricoperta da un rappresentante di AgID o di Consip.
3. I rappresentanti dei Fornitori, presenti alla riunione, hanno facoltà di proporre modifiche o integrazioni nei tempi indicati nella nota di trasmissione, trascorsi i quali senza che nessuna richiesta di modifica sia stata comunicata al segretario e trasmessa per conoscenza a tutti i componenti, il verbale si intende approvato.
4. Le modifiche e integrazioni sono accolte a discrezione di AgID e Consip.
5. L'approvazione del verbale in versione definitiva, a seguito di richieste di modifiche o integrazioni, è comunicata da ciascun componente presente alla riunione a mezzo posta elettronica, salvo quanto previsto ai punti precedenti. A seguito dell'approvazione secondo le modalità sopra indicate, il verbale è firmato digitalmente da AgID e Consip e per presa visione da ciascun componente presente per ogni parte rappresentata ed inviato a mezzo PEC da AgID, con i relativi eventuali allegati, a tutti i componenti. Per esigenze di necessità ed urgenza o comunque per ragioni di interesse pubblico o di norme specifiche, AgID o Consip possono decidere di approvare il verbale anche senza le modifiche/integrazioni proposte dai fornitori.
6. AgID e Consip, in relazione agli argomenti trattati, stabiliscono le forme di pubblicità dei verbali e dei documenti allegati.

#### 4. REGOLAMENTO INTERNO PER IL FUNZIONAMENTO DELL'ORGANISMO STRATEGICO DI COORDINAMENTO E CONTROLLO

##### 4.1 PRINCIPI GENERALI

1. Viene istituito un Comitato Strategico per la governance delle gare strategiche, col fine di garantire l'allineamento complessivo dei contratti e dei progetti rispetto al Piano Triennale per l'informatica nella Pubblica Amministrazione 2020-2022 (e sue successive edizioni), rispetto alle linee guida AgID e alle best practices da quest'ultima individuate ed in coerenza con le previsioni del PNRR.
2. Il Comitato Strategico è così composto:
  - ✓ 1 rappresentante per conto di AgID;
  - ✓ 1 rappresentante per conto di Consip;
  - ✓ 1 rappresentante per conto del Dipartimento per la trasformazione digitale.

##### 4.2 COMPITI E RESPONSABILITÀ DEL COMITATO STRATEGICO

Si riportano di seguito le attività e le responsabilità in capo al Comitato Strategico, fermo restando quanto previsto nella documentazione relativa a ciascuna specifica Gara Strategica:

1. definire l'indicatore del Piano Triennale per l'informatica nella Pubblica Amministrazione 2020-2022 *"R.A.8.1d - Incremento del livello di trasformazione digitale mediante l'utilizzo dei servizi previsti dalle Gare strategiche"*, in particolare, dovrà:
  - a) costruire il livello base dell'indicatore nel 2021, utilizzando un sistema pesato degli indicatori di digitalizzazione delle Gare Strategiche e individuare il valore target per l'anno 2022, nonché gli incrementi attesi annualmente per gli anni successivi;
  - b) a partire dal 2022, con periodicità almeno annuale, raccogliere le misure relative agli indicatori pertinenti e al valore dell'indicatore R.A.8.1d.

Si precisa che alle Gare Strategiche relative alla sicurezza si applica l'indicatore specifico denominato *Indicatore di progresso* nelle modalità definite in documentazione di gara;
2. produrre linee di indirizzo strategico per le Gare Strategiche attive, in predisposizione e per nuove gare volte a soddisfare esigenze di natura strategica, indirizzate nel Piano Triennale per l'informatica o nel PNRR;
3. valutare, trasversalmente a più Gare Strategiche e ai relativi contratti, il livello di aderenza rispetto alle linee strategiche;
4. valutare la coerenza strategica dei contratti esecutivi identificati come *ad alta rilevanza*, risultanti da rilevazioni proprie o segnalati dai Comitati Tecnici o ancora dalle Amministrazioni beneficiarie dei suddetti contratti;
5. garantire la disponibilità di misure (procedurali e/o strumentali) per l'allineamento informativo tra i soggetti coinvolti a vario titolo nelle attività relative alle Gare Strategiche (Comitati Tecnici, Amministrazioni, Fornitori, etc.);

6. valutare ed eventualmente ratificare le proposte di standardizzazione di processi, modelli, soluzioni, metriche, metodologie di stima dei servizi, formulate dai Comitati Tecnici, nel caso di impatti trasversali a più gare strategiche;
7. prendere atto della modalità di revisione dei prezzi e di remunerazione dei servizi, laddove previsto dalla documentazione di gara e formulate secondo le procedure definite ad integrazione del presente regolamento;
8. avviare indagini di soddisfazione delle Amministrazioni per i servizi erogati nell'ambito delle iniziative strategiche, raccogliendone e divulgandone gli esiti;
9. promuovere il riuso di soluzioni e processi tra Amministrazioni, anche avvalendosi delle segnalazioni dei Comitati Tecnici;
10. gestire le escalation segnalate dai Comitati Tecnici.

#### **4.3 RIUNIONI DEL COMITATO STRATEGICO**

1. Il Comitato si riunirà almeno semestralmente;
2. la convocazione potrà essere fatta da uno qualunque dei rappresentanti sopra indicati;
3. la riunione del Comitato Strategico è valida se sono presenti tutti i rappresentanti sopra riportati e prevede la nomina, all'inizio della seduta, di un segretario, cui spetterà la verbalizzazione e le relative attività di invio;
4. nelle riunioni periodiche il Comitato Strategico potrà coinvolgere, al bisogno, una o più Amministrazioni beneficiarie o soggetti istituzionali competenti su specifiche tematiche e/o uno o più fornitori aggiudicatari delle Gare Strategiche.

#### **4.4 ATTI DEL COMITATO STRATEGICO**

1. Gli argomenti discussi nel corso delle riunioni e le decisioni assunte risultano da apposito verbale;
2. il verbale, redatto dal segretario nominato all'inizio della riunione, è trasmesso in versione preliminare a mezzo posta elettronica a tutti i componenti. La funzione di segretario dovrà essere ricoperta da un rappresentante di AgID o di Consip;
3. ogni decisione del Comitato si intende valida se assunta all'unanimità dai rappresentanti di AgID, Consip e del Dipartimento per la trasformazione digitale;
4. fatte salve le indicazioni di legge sulla trasparenza, AgID, Consip e il Dipartimento per la trasformazione digitale, in relazione agli argomenti trattati, stabiliranno le forme di pubblicità degli atti e dei documenti relativi alla governance delle Gare strategiche di volta in volta adottati, ivi incluse ad es. pubblicazioni su siti istituzionali, circolari, studi, etc.

- fine del documento -



**ALLEGATO I – CONTRATTO DI FORNITURA CONTINUATIVA**

**CONTRATTO DI FORNITURA CONTINUATIVA (ex art. 105, comma 3, let. c-bis  
Dlgs. 50/2016)**

**tra**

**Deloitte Risk Advisory S.r.l.**

**e**

**Deloitte Consulting S.r.l.**

## **CONTRATTO DI FORNITURA CONTINUATIVA (ex art. 105, comma 3, let. c-bis Dlgs. 50/2016)**

**tra**

Deloitte Risk Advisory S.r.l., con sede in Milano, Via Tortona, 25 – CAP 20144, iscritta al Registro delle Imprese di Milano Monza Brianza Lodi n./C.F./P.I. 05059250158 ed al R.E.A. di Milano al n. 1105593, in persona dell'Amministratore Delegato Dott. Antonio Arfè, nato a Napoli (RI) il giorno 10 agosto 1973

di seguito per brevità **"Deloitte Risk Advisory"**

**e**

Deloitte & Consulting S.r.l., con sede legale in Milano, Via Tortona, 25 – CAP 20144, iscritta al Registro delle Imprese di Milano Monza Brianza Lodi n./C.F./P.I. 03945320962 ed al R.E.A. di Milano al n. 1713601, nella persona dell'Amministratore Delegato Dott. Alessandro Mercuri, nato a Milano (MI) il giorno 5 marzo 1965 e domiciliato per la carica presso la sede della società,

di seguito, per brevità, denominata anche solo **"DC"** o la **"Parte Fornitrice"**

di seguito congiuntamente per brevità le "Parti" o, singolarmente, la "Parte"

### **Premesso**

- che la Parte Fornitrice è una società che opera nel settore della consulenza alle imprese e svolge, per mezzo della propria organizzazione imprenditoriale, delle proprie risorse e della propria competenza, servizi offerti che riguardano consulenza manageriale Information Technology e supporto operativo alle imprese e alle pubbliche amministrazioni (le **"Aree di Competenza"**);
- che Deloitte Risk Advisory si è avvalsa già in passato, su base temporanea, dei servizi della Parte Fornitrice quale supporto alla propria attività aziendale;
- che entrambe le Parti aderiscono al network internazionale "Deloitte";
- che Deloitte Risk Advisory, anche al fine di rafforzare e potenziare la propria organizzazione aziendale e il servizio offerto, è interessata a richiedere alla Parte Fornitrice l'erogazione, su base stabile e continuativa, di determinati servizi nelle Aree di Competenza a supporto della propria attività aziendale;
- che le Parti intendono pertanto disciplinare in via generale e continuativa la collaborazione che porranno in essere nel periodo di validità del presente accordo di fornitura (di seguito, per brevità, l'**"Accordo"**);
- che l'erogazione dei servizi oggetto del presente Accordo avverrà su richiesta di Deloitte Risk Advisory con le modalità, nei termini e alle condizioni di seguito disciplinati.

**Tutto ciò premesso, le Parti hanno convenuto e stipulato il seguente**

### **CONTRATTO DI FORNITURA CONTINUATIVA**

## **1 EFFICACIA GIURIDICA DELLE PREMESSE E DEGLI ALLEGATI**

- 1.1 Le premesse e gli allegati fanno parte integrante del presente Accordo.
- 1.2 In particolare, costituiscono allegati del presente Accordo:
  - Tariffe standard per la determinazione del corrispettivo (Allegato A);
  - Fac-simile Modello di Richiesta (Allegato B);
  - Fac-simile richiesta di autorizzazione all'affidamento di incarico a collaboratore autonomo e relativa informativa (Allegato C).

## **2 IDONEITÀ TECNICO-PROFESSIONALE DELLA PARTE FORNITRICE**

- 2.1 La Parte Fornitrice dichiara di essere in possesso di pluriennale e consolidata esperienza e specifica professionalità nello svolgimento di servizi di consulenza nelle Aree di Competenza, nonché di strutture ed attrezzature adeguate, e delle licenze/autorizzazioni necessarie, a svolgere compiutamente le attività oggetto del presente Accordo.
- 2.2 La Parte Fornitrice si obbliga ad adeguarsi – entro i termini prescritti – in ipotesi in cui intervengano nuove normative applicabili alle attività per le quali ha dichiarato e comprovato di disporre di licenze e /o autorizzazioni.
- 2.3 L'idoneità tecnico-professionale della Parte Fornitrice costituisce presupposto essenziale del presente Accordo, e il suo venir meno costituisce causa di risoluzione automatica del medesimo. Deloitte Risk Advisory si riserva di verificare il persistere della idoneità tecnico professionale della Parte Fornitrice, nel corso di esecuzione del presente Accordo, mediante l'acquisizione del certificato di iscrizione alla camera di commercio, industria e artigianato dell'impresa, ovvero della relativa autocertificazione.

## **3 OGGETTO E MODALITA' DI ESECUZIONE**

- 3.1 La Parte Fornitrice si impegna ad eseguire a regola d'arte, con propria organizzazione dei mezzi necessari e con gestione a proprio rischio, i servizi che di volta in volta verranno ad essa richiesti per iscritto da Deloitte Risk Advisory utilizzando il modello riportato nell'Allegato B (la "**Richiesta**" o, al plurale, le "**Richieste**"), restando inteso che ciascuna Richiesta sarà soggetta all'accettazione della Parte Fornitrice.
- 3.2 Fermo l'impegno della Parte Fornitrice ad eseguire e realizzare compiutamente e a regola d'arte i servizi di cui alla Richiesta, la stessa Parte Fornitrice sarà comunque libera – fatto salvo quanto previsto al successivo articolo 3.3 – di determinare modalità e termini di esecuzione di tutte le attività che ritenesse utili o necessarie al raggiungimento del miglior risultato finale, coerentemente con quanto indicato da Deloitte Risk Advisory.
- 3.3 La Parte Fornitrice non potrà apportare alcuna modifica o variazione all'oggetto dei servizi di cui alla Richiesta, salvo espressa e preventiva autorizzazione scritta di Deloitte Risk Advisory.
- 3.4 Le modifiche e variazioni di cui al precedente articolo 3.3 non daranno, salvo diverso accordo scritto, diritto ad alcun maggior compenso, anche nel caso di autorizzazione di Deloitte Risk Advisory.
- 3.5 Deloitte Risk Advisory potrà, in qualunque momento, unilateralmente apportare modifiche o variazioni alla Richiesta. La Parte Fornitrice non è tenuta ad accettare variazioni in aumento (intendendosi per tali la durata e l'ampliamento delle attività) ove le stesse non siano state previamente concordate tra le Parti.
- 3.6 Le modifiche e variazioni di cui al precedente articolo 3.5 daranno diritto ad una variazione del corrispettivo, in diminuzione o in aumento rispetto a quanto inizialmente pattuito, in

misura proporzionale al maggior o minor lavoro richiesto dalla fornitura modificata rispetto alla specifica richiesta. La modifica di tale maggiore o minore corrispettivo dovrà essere determinata per iscritto da Deloitte Risk Advisory.

- 3.7 Per singola Richiesta Deloitte Risk Advisory comunicherà la data di inizio dei lavori ed il termine entro il quale gli stessi dovranno essere ultimati. Detto termine deve intendersi essenziale per Deloitte Risk Advisory ai sensi e per gli effetti di cui all'art. 1457 c.c.
- 3.8 La Parte Fornitrice terrà costantemente informata Deloitte Risk Advisory circa l'esecuzione e lo stato dei lavori.
- 3.9 La Parte Fornitrice sarà ad ogni effetto responsabile nei confronti di Deloitte Risk Advisory, nonché, se e per quanto occorrer possa, di ogni terzo interessato, dell'operato dei propri soci e/o dipendenti e/o collaboratori autonomi e/o ausiliari.
- 3.10 Con il presente Accordo, Deloitte Risk Advisory si impegna sin da ora ad acquisire dalla Parte Fornitrice, che si impegna sin da ora ad erogare a favore di Deloitte Risk Advisory, per la durata del presente Accordo un volume minimo di servizi di Euro 50.000,00 (*Euro cinquantamila/00*) con le modalità, nei termini e alle condizioni quivi previste, e fatto comunque salvo quanto previsto al successivo articolo 4. Le Parti danno espressamente atto e convengono che il Volume Iniziale (i) è stato calcolato con riferimento all'intero periodo di durata del presente Accordo, e (ii) dovrà intendersi proporzionalmente ridotto in caso di risoluzione anticipata del presente Accordo per qualsivoglia ragione.

#### **4 DURATA DELL'ACCORDO – PROROGHE – FACOLTÀ DI RECEDERE**

- 4.1 L'Accordo avrà efficacia a far data dalla sua sottoscrizione fino al 31 maggio 2026, al cui scadere cesserà automaticamente di produrre ogni effetto, restando esclusa qualsiasi possibilità di tacita proroga o rinnovazione.
- 4.2 Qualsiasi proroga o rinnovazione dovrà essere concordata tra le Parti, mediante accordo scritto.
- 4.3 Entro il mese di scadenza dell'Accordo, su richiesta indifferentemente di una o dell'altra Parte, le Parti si incontreranno per valutare condizioni e termini di un eventuale rinnovo o proroga dell'Accordo.
- 4.4 Deloitte Risk Advisory potrà recedere anticipatamente ed in qualunque momento dall'Accordo, anche in corso di esecuzione di una specifica Richiesta, con un preavviso di 30 (trenta) giorni. La decisione di recedere dovrà essere comunicata da Deloitte Risk Advisory alla Parte Fornitrice a mezzo lettera raccomandata con avviso di ricevimento. La Parte Fornitrice avrà in tal caso diritto al solo corrispettivo, calcolato sulla base di quanto previsto dal successivo art. 8 e dalla tariffa come da "Allegato A", per l'attività effettivamente svolta fino al termine del periodo di preavviso, unitamente al rimborso delle spese sostenute fino a tale data.
- 4.5 Con il presente Accordo, le Parti espressamente convengono e danno atto che in caso di cessazione del presente Accordo ai sensi del precedente articolo 4.4, e fatto salvo il pagamento del solo corrispettivo maturato ivi previsto, la Parte Fornitrice non avrà diritto ad alcuna indennità, rimborso, contributo e/o risarcimento, anche in deroga all'art. 1671 c.c..

#### **5 RAPPRESENTANTI CONTRATTUALI E TECNICI**

- 5.1 Deloitte Risk Advisory designa il dott. Lorenzo Fersurella quale proprio rappresentante per gli aspetti contrattuali attinenti all'applicazione dell'Accordo (di seguito, "il Rappresentante Contrattuale"), sino a diversa designazione scritta.
- 5.2 La Parte Fornitrice designa il dott. Stefano Alfonso quale proprio Rappresentante Contrattuale, sino a diversa designazione scritta.
- 5.3 Ciascuna Parte nominerà un proprio rappresentante autorizzato in via esclusiva per tutti gli aspetti tecnici (di seguito, "il Responsabile Tecnico"): la nomina del Responsabile Tecnico, che dovrà essere comunicata per iscritto all'altra Parte, avverrà, per quanto riguarda la Parte Fornitrice, nelle specifiche offerte, per quanto riguarda Deloitte Risk Advisory, nelle Richieste di volta in volta emesse.

## **6 VERIFICHE IN CORSO D'OPERA**

- 6.1 Ai sensi di quanto previsto agli artt. 1662 e 1665 c.c., Deloitte Risk Advisory avrà il diritto, in contraddittorio con la Parte Fornitrice, di controllare lo svolgimento dell'attività prestata dalla stessa Parte Fornitrice, al solo fine e nella misura strettamente necessaria alla verifica del corretto adempimento degli obblighi contrattuali assunti dalla Parte Fornitrice, essendo tassativamente escluse forme di direzione, controllo e vigilanza da parte di Deloitte Risk Advisory sui dipendenti e sui collaboratori autonomi della Parte Fornitrice.
- 6.2 Qualora Deloitte Risk Advisory accerti, in contraddittorio con la Parte Fornitrice, che l'esecuzione di alcuno dei servizi non proceda secondo quanto stabilito nell'Accordo e/o nella singola Richiesta, e comunque non a regola d'arte, potrà richiedere alla Parte Fornitrice di conformarsi e/o adempiere correttamente entro il termine di 15 giorni lavorativi dalla comunicazione. Decorso inutilmente tale termine Deloitte Risk Advisory potrà risolvere l'Accordo per inadempimento della Parte Fornitrice, fatto salvo il diritto al risarcimento del danno.

## **7 ACCETTAZIONE DELL'OPERA E GARANZIE**

- 7.1 Ad ogni scadenza prevista nella Richiesta, la Parte Fornitrice consegnerà a Deloitte Risk Advisory la documentazione prevista e concordata quale risultato del lavoro effettuato ovvero darà evidenza del servizio prestato secondo le modalità di volta in volta previste.
- 7.2 I risultati ottenuti sono soggetti ad accettazione da parte del Responsabile Tecnico nominato da Deloitte Risk Advisory sulla base della rispondenza alle specifiche, ai programmi, alle quantità ed alla qualità dei servizi pattuiti con la Parte Fornitrice.
- 7.3 In caso di rifiuto, motivato per iscritto da parte di Deloitte Risk Advisory, dei risultati dell'opera per mancata rispondenza ai requisiti, ovvero di altra contestazione da parte di Deloitte Risk Advisory, la Parte Fornitrice dovrà prontamente porvi rimedio a proprie spese e in ogni caso non oltre quindici giorni di calendario dalla diffida; decorso inutilmente detto termine, l'Accordo potrà essere risolto da Deloitte Risk Advisory per inadempimento della Parte Fornitrice.

## **8 CORRISPETTIVO**

- 8.1 Le Parti concordano che per i servizi di volta in volta commissionati con specifica Richiesta sarà riconosciuto alla Parte Fornitrice un compenso omnicomprendivo. Tale compenso sarà determinato in base ad una stima del tempo e delle risorse impiegate dalla Parte Fornitrice

per la realizzazione dei servizi, secondo le tariffe *standard* di cui all'Allegato A e fermo restando, in ogni caso, quanto previsto dal precedente art. 3.

8.2 Le Parti si danno atto che:

- a) il compenso omnicomprensivo di cui al precedente comma 1 avrà carattere inderogabile;
- b) la durata indicata in ciascuna Richiesta sarà individuata in funzione del tempo stimato per l'ultimazione dei servizi e, pertanto, il termine finale di durata indicata nella Richiesta dovrà essere considerato quale termine di scadenza per l'ultimazione dei servizi;
- c) qualora i servizi richiesti dovessero essere ultimati dopo il termine di scadenza di cui alla relativa Richiesta, e Deloitte Risk Advisory dovesse ugualmente accettarne la consegna, verrà applicata una penale pari al compenso giornaliero per ogni giorno di ritardo fino ad un massimo del 10% del compenso omnicomprensivo di cui al comma 1 del presente articolo. Ai sensi e in conformità dell'art. 1382 c.c. resta salvo il risarcimento del maggior danno. La Parte Fornitrice riconosce l'assoluta importanza, nell'attività imprenditoriale di Deloitte Risk Advisory, delle previsioni del presente articolo e, pertanto, riconosce l'equità dell'importo della penale.
- d) La Parte Fornitrice non può in alcun caso essere considerata inadempiente se il ritardo nella consegna dipende dal fatto di un terzo da cui dipenda in tutto o in parte l'esecuzione del servizio richiesto.

8.3 Resta salva per le Parti la possibilità di modificare, previa stipula di ulteriori accordi scritti, il termine finale di durata indicato nella Richiesta – da intendersi anche quale termine di scadenza per l'ultimazione dei servizi – anche a fronte delle modifiche o variazioni eventualmente richieste da Deloitte Risk Advisory in base al precedente articolo 3.5.

8.4 Le tariffe standard di cui all'Allegato A devono intendersi come comprensive di tutti i costi sostenuti dalla Parte Fornitrice per la corretta e completa effettuazione delle attività richieste da Deloitte Risk Advisory, a qualunque titolo e per qualsiasi causa sostenute.

8.5 Eventuali spese di trasferta sono regolate come da Allegato A

8.6 Resta salva la possibilità di modificare, previa stipula di ulteriori accordi scritti tra le Parti, le stime indicate al precedente articolo 8.1 ovvero di modificare il termine finale di durata indicato nella Richiesta, anche a fronte delle modifiche o variazioni eventualmente richieste da Deloitte Risk Advisory in base al precedente articolo 3.5.

## 9 FATTURAZIONE E PAGAMENTI

9.1 La Parte Fornitrice dovrà emettere le fatture secondo il piano di fatturazione definito nell'Allegato A.

Secondo la normativa vigente sull'obbligo di fatturazione elettronica le fatture dovranno essere emesse ed inviate esclusivamente utilizzando il Sistema di Interscambio (SDI) e secondo il formato (.xml) previsto dalla normativa; di seguito il Codice Destinatario da utilizzare: **UV5W5WD**

Nella descrizione della fattura, la Parte Fornitrice dovrà obbligatoriamente indicare:

- il nominativo e/o email del Responsabile Tecnico nominato da Deloitte Risk Advisory;
- il codice Job/Progetto (qualora previsto).

9.2 Ciascuna fattura dovrà essere accompagnata dalla rendicontazione della tempistica delle attività svolte e delle risorse umane effettivamente impegnate.



- 9.3 Il pagamento della fattura avverrà nei termini e con le modalità di cui all'Allegato A e solo nel caso in cui questa procedura di fatturazione sia eseguita correttamente.
- 9.4 Ogni fattura sarà accompagnata da copia del DURC (Documento Unico di Regolarità Contributiva) in corso di validità.
- 9.5 E' fatto assoluto ed inderogabile divieto alla Parte Fornitrice di emettere tratte per ottenere il compenso di fasi, anche parziali, dei servizi oggetto di una Richiesta o di cedere il credito senza il benestare di Deloitte Risk Advisory.
- 9.6 Anche se emesse, tali tratte non saranno né accettate, né ritirate e la Parte Fornitrice sarà responsabile per i danni derivanti dalla mancata accettazione e/o dal mancato ritiro.

## **10 DIVIETO DI CESSIONE E DI SUBAPPALTO. AUTORIZZAZIONE ALLA PRESTAZIONE D'OPERA**

- 10.1 È fatto assoluto divieto alla Parte Fornitrice di cedere in tutto o in parte l'Accordo, le fatture ed i relativi crediti, nonché di subappaltare, in tutto o in parte, l'esecuzione dei servizi che gli venissero di volta in volta affidati da Deloitte Risk Advisory.
- 10.2 Qualora la Parte Fornitrice ritenesse di dover affidare a collaboratori autonomi l'esecuzione di parte dei servizi oggetto del presente Accordo, prima di procedere dovrà richiedere autorizzazione scritta a Deloitte Risk Advisory mediante invio di richiesta redatta secondo il fac-simile contenuto nell'Allegato C del presente Accordo. La Parte Fornitrice prende atto e accetta espressamente che le valutazioni circa il rilascio o meno dell'autorizzazione sono rimesse al giudizio insindacabile di Deloitte Risk Advisory che non sarà irragionevolmente negato.
- 10.3 Il contratto di collaborazione, inoltre, dovrà contenere clausole che obblighino i collaboratori all'osservanza di obblighi di segretezza/riservatezza, proprietà intellettuale e non concorrenza/non sollecitazione, sostanzialmente conformi a quelli previsti negli articoli 12, 13 e 14 del presente Accordo, nonché il divieto di ulteriore cessione del contratto.
- 10.4 La Parte Fornitrice è responsabile per tutte e ciascuna delle pretese eventualmente avanzate dai propri collaboratori autonomi nei suoi confronti e/o nei confronti di Deloitte Risk Advisory, dando atto a Deloitte Risk Advisory che l'esecuzione dei servizi oggetto del presente Accordo non potrà in alcun modo dar luogo a un rapporto di lavoro subordinato tra la stessa Deloitte Risk Advisory e uno o più collaboratori autonomi della Parte Fornitrice.
- 10.5 La Parte Fornitrice si impegna pertanto a manlevare e tenere indenne Deloitte Risk Advisory da qualsiasi pretesa che i collaboratori autonomi, ancorché da Deloitte Risk Advisory autorizzati, e/o i loro aventi causa, e/o istituti terzi (a titolo esemplificativo INPS, Inail, Agenzia delle Entrate, ecc.) dovessero avanzare nei confronti di Deloitte Risk Advisory in ogni tempo, connessa anche in via indiretta all'esecuzione del presente Accordo ed a rifondere a Deloitte Risk Advisory eventuali danni e/o spese (ivi incluse a titolo esemplificativo e non esaustivo, spese legali, sanzioni, ecc.) sostenute in conseguenza di eventuali pretese e azioni da parte dei predetti soggetti.
- 10.6 La Parte Fornitrice è obbligata e garante dell'avvenuta stipula del relativo contratto e della sottoscrizione da parte del collaboratore autonomo delle clausole sopra richieste, ai sensi del precedente art. 10.3.

## **11 OBBLIGAZIONI DELLA PARTE FORNITRICE**

- 11.1 La Parte Fornitrice opererà in conformità alle specifiche richieste di Deloitte Risk Advisory con i rischi e le responsabilità che la sua qualità di imprenditore gli comporta e, quindi, con organizzazione e gestione di propri mezzi, capitali e risorse, umane e materiali.
- 11.2 La Parte Fornitrice, nell'esecuzione di ciascuna Richiesta, si avvarrà solo di personale con specifica esperienza e competenza, per il quale si impegna ad assolvere le previste normative di legge.
- 11.3 La Parte Fornitrice dichiara e garantisce l'osservanza di tutte le prescrizioni giuridiche e contrattuali in materia di trattamenti retributivi, contributivi, assicurativi e previdenziali nei confronti del personale dipendente e non (ovvero distaccato) di cui si avvale e di attuare e far attuare tutti gli altri adempimenti inerenti ai rapporti di lavoro in conformità ai contratti di categoria in vigore e alle leggi previste dall'ordinamento giuridico italiano. La Parte Fornitrice si impegna inoltre a porre in essere tutte le misure necessarie per garantire la tutela della salute e della sicurezza nei luoghi di lavoro ai sensi del D.Lgs. n. 81/2008 e della normativa di settore e a cooperare con Deloitte Risk Advisory per coordinare ogni azione necessaria per eliminare i rischi dovuti alle interferenze tra i rispettivi lavori. Resta comunque inteso che la Parte Fornitrice sarà l'unico ed il solo soggetto responsabile nei confronti di ogni e qualsivoglia obbligazione nei confronti del personale dipendente e non di cui si avvalga in esecuzione dell'Accordo.
- 11.4 Contestualmente alla sottoscrizione del presente Accordo, la Parte Fornitrice trasmette a Deloitte Risk Advisory copia del DURC in vigore alla data di sottoscrizione dell'Accordo.
- 11.5 Contestualmente all'erogazione del servizio di ogni singola Richiesta, la Parte Fornitrice trasmetterà a Deloitte Risk Advisory copia dei seguenti documenti:
- elenco nominativo del personale dipendente, distaccato nonché dei collaboratori autonomi, impegnati nell'erogazione dei servizi oggetto della Richiesta. La Parte Fornitrice si impegna a tenere costantemente aggiornato detto elenco, comunicando tempestivamente a Deloitte Risk Advisory ogni variazione del medesimo;
  - DURC in vigore alla data della Richiesta, con dichiarazione che i contributi riportati si riferiscono ai lavoratori tutti impiegati nell'esecuzione della Richiesta.
- 11.6 Il Rappresentante Contrattuale individuato dalla Parte Fornitrice ai sensi del precedente art. 5 intratterrà ogni rapporto con Deloitte Risk Advisory, coordinerà e controllerà lo svolgimento del lavoro da parte di tutto il personale di cui si avvarrà la Parte Fornitrice nell'esecuzione delle Richieste, essendo munito di ogni necessario potere al riguardo. Il preposto incaricato dalla Parte Fornitrice dovrà essere sempre presente e/o reperibile durante l'esecuzione del servizio.
- 11.7 Il personale, dipendente o meno, incaricato dalla Parte Fornitrice dell'esecuzione delle Richieste, durante la permanenza presso sedi di Deloitte Risk Advisory o di clienti di quest'ultima, non sarà sottoposto ad alcun potere gerarchico, direttivo e disciplinare da parte di Deloitte Risk Advisory; detto personale dovrà comunque rispettare le disposizioni di sicurezza che regolano l'accesso, la presenza e la circolazione in dette sedi e sarà coperto da opportuna polizza di assicurazione, a cura e spese della Parte Fornitrice.
- 11.8 L'eventuale impedimento per il personale della Parte Fornitrice ad accedere ai locali di Deloitte Risk Advisory o a quelli di clienti di Deloitte Risk Advisory per ferie, festività, cause di forza maggiore, indisponibilità dei locali, non sarà titolo per richiesta di compensi da parte della Parte Fornitrice.
- 11.9 Nel corso dell'esecuzione di una Richiesta, la Parte Fornitrice, previo accordo con il Responsabile Tecnico nominato da Deloitte Risk Advisory, potrà avvicendare il proprio personale, purché di uguale professionalità. Il sostituto si affiancherà al sostituendo per assicurare il necessario passaggio di consegne onde non derivi ritardo nell'esecuzione della

Richiesta. Durante il periodo di affiancamento l'attività del sostituto non avrà effetto sul corrispettivo dovuto per l'esecuzione della Richiesta.

- 11.10 In nessun caso passaggi di categoria o qualifica o variazioni retributive applicati dalla Parte Fornitrice al proprio personale avranno effetto sul corrispettivo.
- 11.11 La Parte Fornitrice è esclusiva responsabile degli adempimenti relativi al proprio personale, dipendente o meno, a tutti gli effetti: retributivo, normativo, previdenziale, assicurativo, fiscale e per ogni altro obbligo che la legge gli imponga.
- 11.12 La Parte Fornitrice si assume ogni e qualsiasi responsabilità per danni a cose o persone derivanti da fatto imputabile a sé, a propri soci e/o dipendenti e/o collaboratori e/o ausiliari incaricati della realizzazione dei servizi.
- 11.13 La Parte Fornitrice si obbliga a manlevare Deloitte Risk Advisory da ogni e qualsivoglia pretesa di risarcimento di qualunque natura e da chiunque avanzata nei confronti della medesima per fatti di cui al punto che precede.
- 11.14 La Parte Fornitrice si impegna, in particolare, a manlevare e tenere indenne Deloitte Risk Advisory da qualsiasi pretesa che il personale dipendente e non della Parte Fornitrice di cui questa si avvarrà per la esecuzione delle Richieste e/o istituti terzi (a titolo esemplificativo INPS, Inail, Agenzia delle Entrate, ecc.) dovessero avanzare nei suoi confronti in ogni tempo, connessa anche in via indiretta all'esecuzione del presente Accordo ed a rifondere a Deloitte Risk Advisory eventuali danni e/o spese (ivi incluse a titolo esemplificativo e non esaustivo, spese legali, sanzioni, ecc.) sostenute in conseguenza di eventuali pretese e azioni da parte dei predetti soggetti.
- 11.15 Le Parti si obbligano a rispettare la disciplina della normativa in materia di *privacy* in quanto applicabile.

## **12 OBBLIGO DI RISERVATEZZA**

- 12.1 La Parte Fornitrice si impegna, anche per i propri soci e/o dipendenti e/o collaboratori e/o ausiliari e/o personale presso il medesimo distaccato, a mantenere strettamente riservati e a non rivelare a terze parti, per tutta la durata dell'Accordo, e comunque per i successivi dieci anni dalla scadenza o risoluzione dell'Accordo, le informazioni, sia relative a Deloitte Risk Advisory che a terzi, nonché quelle relative all'Accordo, di cui sia venuto a conoscenza nell'esecuzione dei servizi concordati (di seguito le "**Informazioni Riservate**").
- 12.2 Le Informazioni Riservate verranno utilizzate dalla Parte Fornitrice nella misura in cui ciò sia strettamente necessario per l'esecuzione dei servizi. La Parte Fornitrice non potrà rilasciare, senza il previo consenso scritto di Deloitte Risk Advisory, comunicati stampa o dichiarazioni a terzi concernenti l'esistenza, l'oggetto e/o i termini dell'Accordo.
- 12.3 Senza limitare la responsabilità della Parte Fornitrice, Deloitte Risk Advisory potrà richiedere, e la Parte Fornitrice si impegna a far sottoscrivere, una dichiarazione di impegno di riservatezza, in conformità ai contenuti inclusi nel presente Articolo, da parte di ogni soggetto (socio e/o dipendente e/o collaboratore e/o ausiliario e/o personale distaccato) che svolge i servizi concordati.
- 12.4 Tale obbligo non si riferisce a dati o informazioni che la Parte Fornitrice possa dimostrare essere stati o divenuti di dominio pubblico, non in violazione del presente obbligo di riservatezza o di ulteriori obblighi di riservatezza nei confronti di terzi.
- 12.5 La proprietà di ogni diritto di proprietà industriale e intellettuale relativo alle informazioni scritte fornite da Deloitte Risk Advisory alla Parte Fornitrice e di tutte le copie, riproduzioni

o parti delle stesse, come pure di qualsiasi oggetto fisico che comprenda le stesse, è e resta di esclusiva proprietà di Deloitte Risk Advisory.

- 12.6 La Parte Fornitrice si impegna a riconsegnare a Deloitte Risk Advisory quanto di sua proprietà al termine dei servizi concordati o in tempo anteriore quando non ne sia più richiesto l'uso per lo svolgimento degli stessi.
- 12.7 La Parte Fornitrice dichiara e garantisce che le informazioni trasmesse a Deloitte Risk Advisory durante l'esecuzione dei servizi concordati non sono soggette a restrizioni d'uso o di rivelazione e la trasmissione a Deloitte Risk Advisory non viola alcun diritto di terzi.
- 12.8 La Parte Fornitrice, qualora non ottemperi agli obblighi di riservatezza di cui al presente articolo, verserà a Deloitte Risk Advisory una penale di € 20.000,00 (*Euro ventimila/00*) per ogni singola violazione, salvo il diritto di Deloitte Risk Advisory al risarcimento del maggior danno. Il pagamento della penale dovrà avvenire entro e non oltre 60 giorni dalla richiesta di Deloitte Risk Advisory, la quale sarà comunicata mediante lettera raccomandata con avviso di ricevimento.

### **13 PROPRIETA' INTELLETTUALE**

- 13.1 La Parte Fornitrice dichiara e garantisce che il prodotto delle attività concordate sarà il risultato di uno sviluppo indipendente ed originale da essa condotto per Deloitte Risk Advisory, esente da violazioni di diritti di brevetto, diritti d'autore, segreti industriali o altri diritti di proprietà industriale o intellettuale di terzi e, in ogni caso, di averne la libera ed incondizionata disponibilità.
- 13.2 La Parte Fornitrice si impegna a difendere a sue spese ed a mantenere indenne Deloitte Risk Advisory, le sue controllanti, le sue consociate ed i suoi clienti, diretti o indiretti, da qualsiasi azione legale che possa essere intrapresa da terzi contro di essi e basata su una tale violazione e da tutti i costi, le spese ed i danni da essi sopportati a seguito di tale azione.
- 13.3 Gli obblighi indicati in questo articolo sopravvivranno all'esaurimento, risoluzione, annullamento o cessazione di ciascuna attività concordata e/o dell'Accordo.
- 13.4 Fatto salvo il diritto alla paternità dell'opera, la Parte Fornitrice conviene che tutti i risultati delle prestazioni commissionate da Deloitte Risk Advisory ed alla stessa fornite sono e restano di proprietà esclusiva di Deloitte Risk Advisory e/o del suo eventuale cliente finale. Il compenso orario pattuito comprende e assorbe qualsiasi diritto della Parte Fornitrice a un corrispettivo per la ideazione dell'opera e la cessione a Deloitte Risk Advisory, a titolo definitivo ed esclusivo, di qualsiasi diritto di proprietà intellettuale.
- 13.5 Deloitte Risk Advisory è proprietaria delle specifiche di prodotto ed ha fornito alla Parte Fornitrice tutte le indicazioni, notizie, nonché i dati sulla base dei quali la Parte Fornitrice ha realizzato i servizi. La Parte Fornitrice, anche per i propri soci e/o dipendenti e/o collaboratori e/o ausiliari e/o personale presso il medesimo distaccato, rinuncia espressamente ad ogni rivendicazione e pretesa nei confronti di Deloitte Risk Advisory o del suo eventuale cliente finale, per quanto attiene il risultato, il prodotto o parti di esso, riconoscendo Deloitte Risk Advisory e/o il cliente finale, a seconda dei casi, quale titolare esclusivo di ogni diritto intellettuale. La Parte Fornitrice si obbliga a non utilizzare in nessun caso in tutto o in parte il risultato e/o il prodotto dei servizi effettuati per Deloitte Risk Advisory in forniture e prestazioni destinate a terzi rispetto a Deloitte Risk Advisory.

### **14 OBBLIGO DI NON CONCORRENZA**

- 14.1 La Parte Fornitrice si impegna a non intraprendere attività professionali direttamente concorrenziali con quelle di Deloitte Risk Advisory in relazione ai servizi oggetto della Richiesta.
- 14.2 L'impegno di cui all'articolo 14.1 è valido per tutta la durata dell'Accordo e per i dodici mesi successivi alla conclusione dello stesso. In caso di anticipato scioglimento dell'Accordo, qualunque ne sia la causa, l'obbligo della Parte Fornitrice sarà valido ed efficace per il più lungo dei due seguenti termini: (i) un termine pari alla durata che avrebbe avuto l'Accordo sulla base delle attività che avrebbe svolto la Parte Fornitrice; (ii) un termine di dodici mesi dalla data di scioglimento dell'Accordo.
- 14.3 I compensi erogati alla Parte Fornitrice in esecuzione del presente Accordo sono comprensivi anche dei corrispettivi per le obbligazioni assunte dalla Parte Fornitrice ai sensi del presente articolo.

## **15 RISOLUZIONE**

- 15.1 Fatto salvo ed impregiudicato quanto previsto nei precedenti articoli, in caso di inadempimento di una delle Parti, l'Accordo e le specifiche richieste emesse in base ad esso può essere considerato risolto dalla Parte non inadempiente a mezzo di comunicazione scritta, qualora l'altra Parte non abbia sanato il proprio inadempimento entro trenta giorni di calendario dal ricevimento della diffida ad adempiere, fermo ogni altro rimedio di legge.
- 15.2 L'Accordo si intende risolto nel caso in cui una delle Parti sia ammessa/richieda o contro di lei sia richiesta l'ammissione a una procedura concorsuale o venga posta in liquidazione.
- 15.3 Ai sensi e per gli effetti disciplinati dall'art. 1456 c.c., Deloitte Risk Advisory potrà risolvere l'Accordo, nonché le specifiche attività ad esso riconducibili in corso di esecuzione, con effetto immediato e per causa imputabile alla Parte Fornitrice, fermo il diritto al risarcimento del danno, qualora la Parte Fornitrice violi una qualsiasi delle seguenti clausole:
- art. 10 (Divieto di cessione e subappalto. Autorizzazione alla prestazione d'opera);
  - art. 11 (Obbligazioni della Parte Fornitrice);
  - artt. 12.1, 12.2, 12.5 e 12.6 (Obbligo di riservatezza);
  - artt. 13.1, 13.2, 13.4 e 13.5 (Proprietà intellettuale);
  - art. 14 (Obbligo di non concorrenza);
  - art. 18 (Responsabilità Amministrativa degli Enti);
  - art. 19.4 (Adempimenti in materia anti-corrruzione).

## **16 LUOGO E FORMA DELLE COMUNICAZIONI**

- 16.1 Le Parti convengono espressamente di riconoscere piena efficacia alle comunicazioni inviate per atto scritto a mezzo posta, telefax e posta elettronica. Tutte le comunicazioni andranno inviate alla sede legale dell'altra Parte e dovranno essere indirizzate al Rappresentante Contrattuale della stessa.

## **17 DISPOSIZIONI GENERALI**

- 17.1 L'Accordo può essere modificato solo per patto scritto firmato da entrambe le Parti.
- 17.2 Ove una delle Parti dell'Accordo non richieda l'esecuzione di uno o più termini, clausole o condizioni contenuti nell'Accordo ciò non potrà essere considerato come rinuncia ad essi o rinuncia alla futura osservanza degli stessi; né la rinuncia ad un qualsiasi termine, clausola o condizione comporterà la rinuncia di un qualsiasi altro termine, clausola o condizione.

- 17.3 I titoli degli articoli contenuti nell'Accordo sono intesi al solo fine di facilitarne la lettura, restando prevalente il contenuto degli articoli stessi.
- 17.4 L'Accordo viene redatto in duplice copia originale, ognuna delle copie avente uguale valore.
- 17.5 All'Accordo sono allegati:
- Allegato A: Tariffe standard;
  - Allegato B: Richiesta;
  - Allegato C: Fac-simile richiesta di autorizzazione all'affidamento di incarico a collaboratore autonomo.

## **18 RESPONSABILITA' AMMINISTRATIVA DEGLI ENTI**

- 18.1 Le Parti si danno reciprocamente atto di aver approvato e formalmente adottato il Modello di Organizzazione, Gestione e Controllo ai sensi del decreto legislativo 8 giugno 2001, n. 231 (D.Lgs. 231/2001) ed il Codice Etico in cui sono enunciati i principi etici ai quali esse si conformano e dei quali viene pretesa la più rigorosa osservanza da parte di tutti coloro che – a qualsiasi titolo – collaborano con esse nel perseguimento dei rispettivi obiettivi.
- 18.1 Le Parti dichiarano di conoscere la normativa di cui al D.Lgs. 231/2001 e di aver preso visione dei rispettivi Codici Etici. Le parti condividono i principi ivi enunciati e intendono pertanto astenersi dall'assumere comportamenti ad essi contrari nello svolgimento delle obbligazioni assunte con la sottoscrizione del presente contratto.
- 18.1 L'eventuale violazione di tali principi etici è considerata quale inadempimento contrattuale e pertanto legittima la parte non adempiente a risolvere il rapporto contrattuale in essere ai sensi e per gli effetti dell'articolo 1456 del c.c., fermo restando il diritto al risarcimento dei danni eventualmente subiti per effetto di detto inadempimento.

## **19 ADEMPIMENTI IN MATERIA ANTI-CORRUZIONE**

- 19.1 Nell'ambito del presente contratto, le Parti si impegnano per sé stesse e per ogni soggetto che, a qualsiasi titolo, agisca in proprio nome e per proprio conto, al rispetto della normativa e dei regolamenti applicabili in tema di prevenzione della corruzione applicabili alle Parti, tra cui a titolo esemplificativo e non esaustivo, U.S. Foreign Corrupt Practices Act e UK Bribery Act (di seguito tutti congiuntamente le "Leggi Anti-corruzione").
- 19.2 Si impegnano a far sì che i propri soci e titolari, dirigenti, dipendenti e agenti e in ogni caso ciascun soggetto che, a qualsiasi titolo, agisca in proprio nome e per proprio conto, comprendano e rispettino tutti gli obblighi di cui al presente articolo, e si impegna altresì a comunicare, tempestivamente e per iscritto, all'altra parte ogni evento o circostanza, in conseguenza del quale gli obblighi sopra indicati non siano più validi e rispettati.
- 19.3 In ipotesi di avvio di qualsivoglia indagine, da parte dell'autorità giudiziaria o di altra autorità di vigilanza, volta ad accertare la violazione delle Leggi Anti-corruzione, nella quale sia coinvolta una parte, l'altra parte avrà facoltà di recedere liberamente dal presente contratto, mediante comunicazione scritta da inviarsi a mezzo di raccomandata A/R, ovvero comunicazione equipollente, con un preavviso di 15 (quindici) giorni, senza che sia tenuta a corrispondere alcun importo a nessun titolo, fatto salvo il corrispettivo dovuto per le prestazioni eventualmente già eseguite.
- 19.4 Il presente contratto si risolverà, ai sensi e per gli effetti di cui all'articolo 1456 c.c., nel caso di violazione delle Leggi Anti-corruzione, accertata in via definitiva da parte dell'autorità giudiziaria o di altra autorità di vigilanza.

- 19.5 Le Parti si riservano, altresì, il diritto di riformulare il presente articolo in caso di modifica delle Leggi Anti-corruzione, dandone comunicazione all'altra parte, la quale si impegna ad accettare le modifiche apportate in applicazione del presente articolo.

## **20 PROTEZIONE DEI DATI PERSONALI**

- 20.1 Nella presente clausola, per "Disciplina in materia di protezione dei dati personali" s'intendono: (i) il Regolamento generale dell'UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché della libera circolazione di tali dati ("Regolamento"); e (ii) ogni ulteriore legge, atto avente forza di legge e/o regolamento in materia di protezione dei dati personali applicabile.

I termini di seguito elencati avranno il significato agli stessi attribuito nella presente clausola e nella Disciplina in materia di protezione dei dati personali:

- ✓ "dati personali": qualsiasi informazione riguardante una persona fisica identificata o identificabile. I dati personali che la Parte Fornitrice tratta per conto di Deloitte Risk Advisory sono ricompresi nelle seguenti categorie: Dati personali comuni, Dati personali sensibili, intesi come categorie particolari di dati personali, Dati personali giudiziari;
- ✓ "categorie particolari di dati personali": dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
- ✓ "persona interessata": una persona fisica identificata o identificabile. Gli interessati i cui dati personali sono trattati dalla Parte Fornitrice per conto di Deloitte Risk Advisory sono ricompresi nelle seguenti categorie: clienti/dipendenti/collaboratori del/i cliente/i di Deloitte Risk Advisory, ove previsti, dipendenti/collaboratori di Deloitte Risk Advisory ove previsti;
- ✓ "titolare del trattamento": la persona fisica o giuridica, l'autorità pubblica o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- ✓ "responsabile del trattamento": la persona fisica o giuridica, l'autorità pubblica o altro organismo che tratta dati personali per conto del titolare del trattamento;
- ✓ "sub-responsabile del trattamento": la persona fisica o giuridica, l'autorità pubblica o altro organismo che tratta dati personali per conto di un altro responsabile del trattamento;
- ✓ "trattamento": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

- 20.2 Deloitte Risk Advisory, in qualità di titolare del trattamento dei dati personali, per i dati personali trattati nel proprio interesse, o di responsabile del trattamento per i dati personali trattati nell'interesse di un proprio cliente o di più clienti, nell'ambito del presente Accordo, nomina la Parte Fornitrice rispettivamente responsabile del trattamento per i dati personali trattati nell'interesse di Deloitte Risk Advisory o sub responsabile del trattamento dei dati personali trattati nell'interesse di un cliente o di più clienti di Deloitte Risk Advisory, che



accetta. Deloitte Risk Advisory ricorre alla Parte Fornitrice come responsabile o sub-responsabile per l'esecuzione di specifiche attività di trattamento, la quale garantisce l'adozione di misure tecniche e organizzative adeguate affinché ogni trattamento soddisfi i requisiti previsti dalla Disciplina in materia di protezione dei dati personali.

20.3 La Parte Fornitrice terrà indenne Deloitte Risk Advisory dalle conseguenze derivanti (i) da ogni eventuale inadempimento da parte della stessa Parte Fornitrice, dei suoi dipendenti e/o collaboratori e/o ausiliari e/o del personale distaccato degli obblighi che su di esso gravano in virtù della Disciplina in materia di protezione dei dati personali e di quanto previsto dalla presente clausola; (ii) da qualsiasi azione od omissione della Parte Fornitrice, dei suoi dipendenti e/o collaboratori e/o ausiliari e/o del personale distaccato da cui derivi a qualsiasi titolo una responsabilità di Deloitte Risk Advisory nei confronti della persona interessata.

20.4 Sia Deloitte Risk Advisory che la Parte Fornitrice si impegnano ad adempiere gli obblighi che su di essi rispettivamente gravano in virtù della Disciplina in materia di protezione dei dati personali con specifico riferimento ai dati personali che ciascuno rispettivamente tratta nell'ambito del presente Accordo e ai fini dei servizi di cui al presente Accordo (di seguito "Servizi").

20.5 La Parte Fornitrice:

20.5.1 tratterà i dati personali, anche in modalità elettronica, esclusivamente: (i) nella misura necessaria per la prestazione dei Servizi; (ii) nel rispetto delle istruzioni specifiche impartite da Deloitte Risk Advisory salvo che, a giudizio della Parte Fornitrice, tali istruzioni violino la Disciplina in materia di protezione dei dati personali e/o altre disposizioni con efficacia di legge, circostanza di cui la Parte Fornitrice informerà Deloitte Risk Advisory; (iii) secondo quanto previsto dalle autorità competenti e/o dalla Disciplina in materia di protezione dei dati personali applicabile;

20.5.2 adotterà le opportune misure tecniche e organizzative in conformità alle previsioni normative applicabili, ed in particolare alle disposizioni di cui all'art. 32 del Regolamento, tra cui ove necessario l'adozione di misure di pseudonimizzazione e cifratura dei dati e quelle in grado di ripristinare tempestivamente la disponibilità e l'accesso dei Dati Personali in caso di incidente fisico o tecnico per garantire un livello di sicurezza commisurato al rischio associato al trattamento operato in qualità di responsabile o sub-responsabile del trattamento dei dati personali, ivi inclusi eventuali requisiti di sicurezza ed eventuali ulteriori specifiche misure di sicurezza indicate, come anche nell'ambito dei programmi di certificazione ISO 27001/27002 ove sussistenti;

20.5.3 manterrà, e farà in modo che: (i) ogni soggetto autorizzato dalla Parte Fornitrice al trattamento dei dati personali ovvero (ii) i suoi dipendenti e/o collaboratori autonomi e/o ausiliari e/o personale distaccato a cui dovesse venire affidata parte dell'esecuzione delle attività di cui al presente Accordo, a seguito di autorizzazione di Deloitte Risk Advisory, si impegnino a rispettare:

(a) specifici obblighi di confidenzialità previsti nel presente Accordo;

(b) la Disciplina in materia di protezione dei dati personali;

20.5.4 dopo esserne venuto a conoscenza, darà tempestiva comunicazione a Deloitte Risk Advisory di ogni eventuale violazione dei dati personali del cui trattamento la Parte Fornitrice è responsabile o sub-responsabile e presterà ad esso l'opportuna collaborazione;

20.5.5 fornirà a Deloitte Risk Advisory l'opportuna collaborazione e assistenza relativamente (i) alla predisposizione di valutazioni di impatto dei trattamenti effettuati sulla protezione dei dati Personali, (ii) a eventuali richieste di consultazioni preventive all'autorità di controllo qualora la valutazione d'impatto presenti un rischio elevato per la protezione dei dati personali (iii) a eventuali richieste, da parte di una persona interessata, di accesso ai dati personali del cui trattamento la Parte Fornitrice è

responsabile o sub-responsabile, ovvero in relazione ad eventuali richieste di informazioni, pronunce ovvero segnalazioni da parte di un'autorità competente, ovvero di una persona interessata rivolte a Deloitte Risk Advisory; la Parte Fornitrice comunicherà altresì per iscritto tempestivamente a Deloitte Risk Advisory la circostanza in cui abbia a propria volta ricevuto richieste di informazioni da parte di un'autorità competente, ovvero di una persona interessata, salvo nella misura in cui tale comunicazione risulti vietata in base alla normativa applicabile;

20.5.6 fermo restando quanto previsto dal successivo comma 8 della presente clausola e previa richiesta ragionevole di Deloitte Risk Advisory, cancellerà ovvero restituirà a Deloitte Risk Advisory i dati personali trattati allo scioglimento ovvero alla scadenza del rapporto contrattuale con quest'ultimo;

20.5.7 La Parte Fornitrice si impegna a manlevare e tenere indenne Deloitte Risk Advisory da qualsiasi pretesa avanzata da persone interessate in relazione all'eventuale violazione delle presenti clausole da parte della Parte Fornitrice e dei suoi dipendenti e/o collaboratori autonomi e/o ausiliari e/o personale distaccato.

20.6 Secondo quanto previsto dalla Disciplina in materia di protezione dei dati personali applicabile, la Parte Fornitrice conserverà un registro delle attività di trattamento che svolge in qualità di responsabile o sub-responsabile. La Parte Fornitrice potrà altresì permettere a Deloitte Risk Advisory di svolgere, esclusivamente a proprie spese, una attività di audit nei riguardi della stessa Parte Fornitrice, al fine di valutare la conformità del trattamento dei dati posto in essere da quest'ultimo a quanto previsto dalla presente clausola e alle istruzioni impartite da Deloitte Risk Advisory, purché siano soddisfatte le seguenti condizioni e fatto salvo quanto altrimenti eventualmente espressamente previsto dalle autorità competenti:

20.6.1 Deloitte Risk Advisory comunicherà per iscritto con almeno 30 giorni di preavviso l'intenzione di porre in essere un'attività di audit ai sensi della presente clausola e ne concorderà con la Parte Fornitrice in buona fede l'oggetto e i parametri di riferimento;

20.6.2 qualora: (i) l'oggetto dell'attività di *audit* di cui al punto precedente coincida con l'oggetto di una attività di *audit* cui la Parte Fornitrice è stato sottoposto da parte di un terzo indipendente nei dodici mesi precedenti alla richiesta di Deloitte Risk Advisory di cui alla presente clausola; e (ii) i presidi posti a tutela dei dati personali da parte della Parte Fornitrice non abbiano subito variazioni sostanziali nel corso di tale periodo, la Parte Fornitrice potrà condividere con Deloitte Risk Advisory la relazione emessa a conclusione di tale attività di *audit* svolta dal terzo indipendente, nella misura rilevante e pertinente, restando inteso che in tal modo la richiesta di Deloitte Risk Advisory di cui alla presente clausola potrà essere ritenuta soddisfatta; laddove però Deloitte Risk Advisory ritenesse tali controlli non soddisfacenti o comunque Deloitte Risk Advisory, a suo insindacabile giudizio, ritenesse necessario procedere ad una nuova attività di controllo per verificare il rispetto degli obblighi a cui è tenuto la Parte Fornitrice, la stessa Deloitte Risk Advisory potrà anche tramite propri soggetti incaricati svolgere attività di controllo nei confronti di quest'ultimo;

20.6.3 in ogni caso, l'eventuale attività di *audit* sarà svolta da Deloitte Risk Advisory durante il normale orario di operatività della Parte Fornitrice, nel rispetto delle relative policy e con l'impegno ad interferire con le attività svolte dalla Parte Fornitrice nella misura strettamente indispensabile a permetterne lo svolgimento;

20.6.4 l'attività di *audit* di cui alla presente clausola sarà in ogni caso svolta da Deloitte Risk Advisory nel rispetto degli obblighi di riservatezza che la Parte Fornitrice assume, in

particolare nei confronti dei propri clienti, associati e dipendenti, e non potrà in alcun caso riguardare le attività svolte dai suoi sub-contrattanti;

20.6.5 l'attività di *audit* di cui alla presente clausola non potrà essere svolta più di una volta nel corso di un anno solare.

20.7 La Parte Fornitrice non potrà comunicare i dati personali a terzi, salvo le autorità competenti, né potrà avvalersi di sub-responsabili del trattamento, salvo che non sia a ciò preventivamente autorizzato da Deloitte Risk Advisory per iscritto.

20.8 Deloitte Risk Advisory riconosce che la Parte Fornitrice, oltre a trattare dati personali in qualità di responsabile o sub-responsabile ai sensi della presente clausola, potrà altresì trattare dati personali in qualità di titolare con riferimento a: (i) obblighi imposti da leggi, regolamenti e/o atti aventi forza di legge applicabili; (ii) richieste di informazioni e/o comunicazioni da parte delle autorità competenti; e (iii) finalità di natura amministrativa, di contabilità, di analisi dei rischi.

20.9 La Parte Fornitrice s'impegna a fornire ai propri collaboratori a cui affida l'esecuzione delle attività di cui al presente Accordo, a seguito di autorizzazione di Deloitte Risk Advisory ove necessaria, l'informativa sub Allegato C con cui gli stessi sono informati del trattamento effettuato da Deloitte Risk Advisory, in qualità di titolare, relativo ai loro dati personali.

## **21 LEGGE APPLICABILE - FORO COMPETENTE**

21.1 Il presente accordo è regolato dalla legge italiana.

21.2 Le Parti stabiliscono che per qualsiasi controversia derivante o comunque connessa all'Accordo ovvero alla singola Richiesta sarà esclusivamente competente il Foro di Milano.

Letto, confermato e sottoscritto in Roma, il 19 aprile 2021

**Deloitte Risk Advisory S.r.l.**  
**Amministratore Delegato**

**La Parte Fornitrice**  
**Deloitte Consulting S.r.l.**

Ai sensi e per gli effetti disciplinati dagli artt. 1341 e 1342 c.c., si approvano espressamente le seguenti clausole:

3 (OGGETTO E MODALITA' DI ESECUZIONE), 4 (DURATA - PROROGHE - FACOLTÀ DI RECEDERE), 7 (ACCETTAZIONE DELL'OPERA E GARANZIE), 10 (DIVIETO DI CESSIONE E DI SUBAPPALTO. AUTORIZZAZIONE ALLA PRESTAZIONE D'OPERA), 11 (OBBLIGAZIONI DELLA PARTE FORNITRICE), 12 (OBBLIGO DI RISERVATEZZA), 13 (PROPRIETÀ INTELLETTUALE), 14 (OBBLIGO DI NON CONCORRENZA), 15 (RISOLUZIONE), 18 (RESPONSABILITÀ AMMINISTRATIVA DEGLI ENTI), 19 (ADEMPIMENTI IN MATERIA ANTI-CORRUZIONE), 20 (PROTEZIONE DEI DATI PERSONALI), 21 (LEGGE APPLICABILE - FORO COMPETENTE).

Roma, il 19 aprile 2021

**La Parte Fornitrice**  
**Deloitte Consulting S.r.l.**



## Allegato A

### Tariffe standard per la determinazione del corrispettivo

<b>Tariffe giornaliere CONTRATTO DI FORNITURA DI SERVIZI</b>	
<b>Profilo</b>	<b>Tariffa giornaliera</b>
Capo progetto	600 €/giorno
Manager	500 €/giorno
Senior	400 €/giorno
Junior	300 €/giorno
Specialista	550 €/giorno

<b>Note sui rate applicati</b>
Rate riferiti ad una giornata media di 8 ore

<b>Descrizione Profili</b>
Junior 1: fino a 4 anni di esperienza
Senior: da 4 a 6 anni di esperienza
Manager: da 6 a 10 anni di esperienza
Capo progetto: oltre 10 anni di esperienza
Specialista: almeno 6 anni di esperienza specifica

Tariffa giornaliera Standard: giornata lavorativa di 8 ore tra le 09.00 e le 18.00, dal lunedì al venerdì inclusi.

La maggiorazione prevista per le ore lavorate nei giorni festivi, oppure oltre le ore 18.00 di qualunque giorno è pari al 20%.

Le tariffe sopra riportate sono da considerarsi onnicomprensive a parte gli oneri, a carico di Deloitte Risk Advisory, relativi all'IVA.

Nessun rimborso spese sarà dovuto da Deloitte Risk Advisory alla Parte Fornitrice, restando a carico di quest'ultimo tutte le spese sostenute in relazione all'esecuzione della Richiesta ed essendo espressamente convenuto che il compenso è stato determinato nella misura sopra indicata anche perché comprensivo di un rimborso spese a carattere forfetario.

La fatturazione dei corrispettivi, avrà in linea di principio cadenza mensile.

Il pagamento dei corrispettivi avverrà a 90 giorni data fattura ovvero prima se fosse precedente la data del pagamento della fattura da parte del Committente finale, a condizione che, nel frattempo, siano stati consegnati i documenti di cui all'articolo 9.4 del presente Accordo,

## **Allegato B – Fac-simile**

### **Modello di Richiesta**

In riferimento al contratto di fornitura continuativa stipulato in data [●], Deloitte Risk Advisory S.r.l. con il presente documento emette la seguente

#### **RICHIESTA DI OFFERTA DI CONSULENZA Nr. .... del .....**

Oggetto		
Descrizione delle attività oggetto di incarico di consulenza		
Responsabile Tecnico		
nr. job Deloitte Risk Advisory		
Durata prevista	dal	al
Compenso omnicomprensivo	EUR ..... ( <i>Euro –in lettere</i> )	
Modalità di pagamento		
Altro/note		

**Deloitte Risk Advisory S.r.l.**  
**Amministratore Delegato**

Per accettazione  
La Parte Fornitrice

---

---

## Allegato C – Fac-simile

(in caso di mancata consegna contestuale alla sottoscrizione della Richiesta, ai sensi dell'art. 11.5, si prega di inviare la presente comunicazione a:)

Deloitte Risk Advisory S.r.l.  
Central Talent Office  
Via Tortona, 33  
20144 MILANO

### **Richiesta di Autorizzazione all'affidamento di incarico a collaboratore autonomo e relativa informativa**

Il/La sottoscritto/a ..... nella qualità di legale rappresentante della società ....., (di seguito la Parte Fornitrice) ai sensi dell'art. 10 del contratto di fornitura continuativa stipulato con **Deloitte Risk Advisory** e sottoscritto in data ..... (di seguito semplicemente "Accordo")

### **C h i e d e**

Che il Sig. ....(di seguito "Collaboratore") nato a .....il....., CF ....., P. IVA ....., residente in ..... alla via .....n ....., con studio/domicilio professionale in ..... alla via .....n ....., in possesso della seguente qualifica/titolo professionale .....(qualora il soggetto sia iscritto ad un albo professionale indicare quale e la data di iscrizione ..... ) sia autorizzato all'esecuzione di servizi oggetto della Richiesta n ..... del \_\_\_/\_\_\_/\_\_\_ emessa da parte di Deloitte Risk Advisory ai sensi dell'art. 3.1 del suddetto Accordo.

Il sottoscritto si obbliga, anche ai sensi e per gli effetti di cui all'art. 10.6 dell'Accordo sottoscritto con Deloitte Risk Advisory, a stipulare, con il predetto Collaboratore, un contratto che contenga le clausole comprendenti gli obblighi espressamente previsti dall'art. 10.3 dell'Accordo.

Il sottoscritto si impegna a comunicare tempestivamente a Deloitte Risk Advisory eventuali variazioni dei dati sopra indicati del Collaboratore, ovvero la cessazione o risoluzione del contratto di collaborazione stipulato.

Si dichiara, infine, di avere fornito al Collaboratore l'informativa al trattamento dei dati personali allegata alla presente.

Luogo e Data

\_\_\_\_\_, \_\_\_/\_\_\_/\_\_\_\_\_

La Parte Fornitrice  
[denominazione]

\_\_\_\_\_  
(Il Legale Rappresentante)

\_\_\_\_\_  
(spazio da compilare a cura di Deloitte Risk Advisory)

PRESA VISIONE DELLA SUDETTA RICHIESTA, Deloitte Risk Advisory AUTORIZZA L'ESECUZIONE DEGLI INCARICHI DA PARTE DEL COLLABORATORE SOPRA INDICATO, ESPRESSAMENTE DELEGATO DALLA PARTE FORNITRICE E NEI LIMITI DEGLI INCARICHI ASSEGNATI.

MILANO, IL \_\_\_\_\_



## **Informativa ai sensi del Regolamento EU 679/2016 relativa alla richiesta di autorizzazione all'affidamento di incarico a collaboratore autonomo**

Ai sensi dell'art. 14 del Regolamento Europeo (EU) 679/2016 relativo alla protezione dei dati personali ("Regolamento") e della normativa nazionale, compresi i singoli provvedimenti dell'Autorità di controllo, Garante per la protezione dei dati personali, ove applicabile, Le comunichiamo, nella Sua qualità di Interessato, che Deloitte Risk Advisory ha ricevuto dalla Deloitte Consulting S.r.l. dati a Lei relativi, qualificati come personali dal predetto Regolamento e che, pertanto, la stessa è tenuta, in qualità di Titolare del trattamento, a fornirLe alcune informazioni riguardanti il trattamento degli stessi Suoi dati.

Si specifica che per "trattamento" di dati personali, ai sensi del Regolamento, si intende qualsiasi operazione o insieme di operazioni, compiute da Deloitte Risk Advisory con o senza l'ausilio di processi automatizzati e applicate ai Suoi dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

### **1. Titolare e Responsabile del trattamento dei dati personali**

Il titolare del trattamento dei Dati Personali è Deloitte Risk Advisory S.r.l., con sede legale in Milano, via Tortona 25 (in seguito "Deloitte Risk Advisory").

Il responsabile della protezione dei dati personali individuato da Deloitte Risk Advisory è Tommaso Stranieri, contattabile al seguente indirizzo e-mail: [dataprotectionofficer@deloitte.it](mailto:dataprotectionofficer@deloitte.it)

### **2. Natura dei dati trattati, finalità e base giuridica del trattamento**

Sono oggetto di trattamento i Suoi dati personali, ove per dato personale si intende qualunque informazione a Lei relativa quale persona fisica, identificata o identificabile anche indirettamente mediante riferimento a qualsiasi altra informazione ("Interessato"), comunicati a Deloitte Risk Advisory dalla Società Deloitte Consulting S.r.l., (di seguito "Società") in occasione della richiesta di autorizzazione all'affidamento di incarico a collaboratore autonomo nell'ambito del contratto stipulato tra Deloitte Risk Advisory e la Società in data \_\_\_\_\_.

I dati personali trattati da Deloitte Risk Advisory saranno utilizzati esclusivamente al fine di: (i) essere informata in merito al Suo percorso di formazione e professionale, in vista del rapporto contrattuale con la Società (ii) evitare la prestazione di servizi in contrasto con la normativa vigente in materia di indipendenza, (iii) evitare l'insorgenza di conflitti di interesse, (iv) adempiere agli obblighi di legge.

Il consenso al trattamento dei dati personali per le finalità suddette non occorre poiché i dati vengono raccolti per l'adempimento di obblighi legislativi, tra cui quelli sull'indipendenza e assenza di conflitti di interesse.

La base giuridica del trattamento è costituita dall'esecuzione di misure precontrattuali e dall'adempimento di obblighi di legge.

### **3. Modalità del trattamento**

I Suoi dati personali sono raccolti in via cartacea, sono trattati con l'ausilio di strumenti elettronici e manualmente, assicurando l'impiego di misure idonee per la sicurezza dei dati trattati e garantendo la riservatezza dei medesimi, in conformità ai principi applicabili al trattamento di dati personali ai sensi dell'art. 5 del Regolamento, quali liceità, correttezza e trasparenza, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza.

### **4. Durata del trattamento**

I Suoi dati saranno conservati per il periodo normativamente previsto in ottemperanza agli obblighi di natura civilistica, fiscale e tributaria vigenti, nonché per esercitare o difendere un diritto in sede giudiziaria e comunque per massimo 10 anni decorrenti dal conferimento degli stessi a Deloitte Risk Advisory.

## **5. Comunicazione e trasferimento dei dati**

Con riferimento alle finalità sopra indicate, Deloitte Risk Advisory potrà comunicare i Suoi dati personali a:

- altre Società del Network Deloitte Risk Advisory qualora necessario per il perseguimento delle finalità sopra indicate, per lo svolgimento di attività di amministrazione interna, strumentali, connesse o di supporto a quella di Deloitte Risk Advisory;
- soggetti terzi incaricati dal titolare per l'espletamento dei servizi connessi alle attività svolte, anche di revisione contabile se prevista;
- autorità competenti (inclusi tribunali), per lo svolgimento delle loro funzioni istituzionali nei limiti stabiliti da legge o regolamenti.

I dati sono comunicati a soggetti terzi previa opportuna designazione nel ruolo di Responsabili del trattamento o, in caso diverso, a seguito del riconoscimento di una Titolarità autonoma.

I dati personali verranno trattati da collaboratori e/o dipendenti di Deloitte Risk Advisory nell'ambito delle rispettive funzioni ed in conformità alle istruzioni impartite dalla stessa Deloitte Risk Advisory. In particolare, potranno altresì avere accesso ai Suoi Dati le seguenti categorie di incaricati:

- addetti alla contabilità;
- addetti all'ufficio del personale;
- addetti che si occupano di effettuare gli adempimenti previsti dalla normativa antiriciclaggio, anticorruzione nonché le verifiche sull'indipendenza e assenza di conflitti di interessi di Deloitte Risk Advisory.

Se necessario per i fini sopra indicati, le informazioni raccolte saranno trasmesse o rese accessibili ad altre Società del Network di Deloitte Risk Advisory, aventi sede anche in Paesi non appartenenti all'Unione Europea. In tali casi, il titolare garantisce l'adozione di adeguate misure che assicurino un livello di protezione dei dati conforme agli obblighi a cui esso è giuridicamente tenuto, quali il ricorso alle clausole contrattuali standard per il trasferimento di dati personali in Paesi Terzi.

I Suoi dati personali non saranno oggetto di diffusione.

## **6. Diritti dell'interessato**

L'interessato potrà esercitare, in relazione al trattamento dei dati ivi descritto e compatibilmente con le necessità di trattamento indicate nella presente informativa, i seguenti i seguenti diritti previsti dal Regolamento (artt.15-21):

- ricevere conferma dell'esistenza dei suoi dati personali e accedere al loro contenuto (diritto di accesso);
- aggiornare, modificare e/o correggere i suoi dati personali (diritto di rettifica);
- chiederne la cancellazione o la limitazione del trattamento dei dati trattati in violazione di legge compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o altrimenti trattati (diritto all'oblio e diritto alla limitazione);
- opporsi al trattamento (diritto di opposizione);
- revocare il consenso, ove prestato, senza pregiudizio per la liceità del trattamento basata sul consenso prestato prima della revoca;
- proporre reclamo all'Autorità di controllo in caso di violazione della normativa in materia di protezione dei dati personali;
- ricevere copia dei dati che lo riguardano in formato elettronico e chiedere che tali dati siano trasmessi ad un altro titolare del trattamento (diritto alla portabilità dei dati).

Per esercitare tali diritti l'interessato potrà rivolgersi al responsabile della protezione dei dati inviando un'e-mail a [dataprotectionofficer@deloitte.it](mailto:dataprotectionofficer@deloitte.it)