SISTEMA SANITARIO REGIONALE
ASL ROMA 1

DELIBERAZIONE DEL DIRETTORE GENERALE

N. 262 **del** 03/03/2023

OGGETTO: Adesione all'Accordo Quadro Consip "SERVIZI DI SICUREZZA DA REMOTO, COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI - Lotto 2" (Cig madre 8884642E81) - SSN - ID 2296" con il Fornitore RTI Deloitte Risk Advisory S.r.l. (Mandataria), per la l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni per le esigenze della Asl Roma 1 - Importo complessivo pari ad € 2.272.327,70 iva esclusa, comprensivi delle quote per incentivi funzioni tecniche (€ 2.770.660,69 iva inclusa) per un periodo di 36 mesi. (CIG Derivato 9668894FBA).

STRUTTURA PROPONENTE: DIPARTIMENTO TECNICO PATRIMONIALE - UOC SISTEMI E TECNOLOGIE INFORMATICHE DI COMUNICAZIONE

Centro di Costo: BD07 L'Estensore: SERENA SBRIGLIO Il presente Atto non contiene dati sensibili

Il Dirigente e/o il Responsabile del procedimento, con la sottoscrizione del presente atto, a seguito dell'istruttoria effettuata, attestano che l'atto è legittimo nella forma e nella sostanza.

Il Responsabile del Procedimento	UOC SISTEMI E TECNOLOGIE INFORMATICHE DI COMUNICAZIONE	DIPARTIMENTO TECNICO PATRIMONIALE
Ing. DEBORA ANGELETTI	Ing. DEBORA ANGELETTI	Ing. PAOLA BRAZZODURO
Firmatario: DEBORA ANGELETTI Data: 21/02/2023 13:12:41 CET	Firmatario: DEBORA ANGELETTI Data: 21/02/2023 13:18:36 CET	Firmatario: PAOLA BRAZZODURO Data: 23/02/2023 11:09:40 CET

Il funzionario addetto al controllo di budget, con la sottoscrizione del presente atto, attesta che lo stesso non comporta uno scostamento sfavorevole rispetto al budget economico assegnato come di seguito dettagliato per singolo conto:

Costo previsto	Eserciz.	CE/CP	Numero conto	Descrizione conto	Addetto al controllo	Scostamento
€7.177,70	2023	CE	516040605	accantonamento incentivi funzioni tecniche art. 113 d.lgs. 50/2016	Ing. Debora Angeletti	No
€906.521,00	2023	CE	502020106	Servizi di assistenza informatica	Ing. Debora Angeletti	No
€1.167.601,00	2024	CE	5202020106	Servizi di assistenza informatica	Ing. Debora Angeletti	No
€689.361,00	2025	CE	502020106	Servizi di assistenza informatica	Ing. Debora Angeletti	No

Il Funzionario addetto al controllo di budget

Ing. DEBORA ANGELETTI

Firmatario: DEBORA ANGELETTI
Data: 21/02/2023 13:20:44 CET

Il Dirigente della UOC Pianificazione Strategica, Programmazione e Controllo di Gestione con la sottoscrizione del presente atto attesta la coerenza della dichiarazione riferita alla spesa, di cui al presente provvedimento del "funzionario addetto al controllo del budget", rispetto alla delibera n.23 del 17/01/2023.

Il sostituto MADDALENA QUINTILI
Data: 01/03/2023 16:19:34 CET

Parere del Direttore Amministrativo Dr.ssa Roberta Volpini

Favorevole

Firmatario: ROBERTA VOLPINI
Data: 02/03/2023 15:23:08 CET

(con motivazioni allegate al presente atto)
Non favorevole

Parere del Direttore Sanitario Dr. Gennaro D'Agostino

Favorevole

Firmatario: GENNARO D'AGOSTINO
Data: 02/03/2023 16:24:03 CET

(con motivazioni allegate al presente atto)
Non favorevole

Il presente provvedimento si compone di n.53 pagine di cui n. 43 pagine di allegati

Il Direttore Generale f.f.
Dr.ssa Roberta Volpini

Firmatario: ROBERTA VOLPINI
Data: 03/03/2023 11:20:02 CET

REGIONE LAZIO

IL DIRETTORE DELLA U.O.C. SISTEMI E TECNOLOGIE INFORMATICHE E DI COMUNICAZIONE

VISTA la deliberazione del Commissario Straordinario n. 1 del 1° gennaio 2016, con la quale si è provveduto a prendere atto dell'avvenuta istituzione dell'Azienda Sanitaria Locale Roma 1 a far data dal 1° gennaio 2016, come previsto dalla legge regionale n. 17 del 31.12.2015 e dal DCA n. 606 del 30.12.2015;

VISTA la Deliberazione del Direttore Generale n. 620 del 22/09/2022 avente ad oggetto: "Cessazione del Dr. Angelo Tanese dall'incarico di Direttore Generale della ASL Roma 1 e contestuale individuazione del Direttore Amministrativo Aziendale, D.ssa Roberta Volpini quale facente funzioni";

VISTO l'Atto di Autonomia Aziendale, approvato con deliberazione n. 1153 del 17/12/2019, recepito con DCA U00020 del 27/01/2020, pubblicato sul BURL del 30/01/2020 n. 9 con il quale, tra l'altro, è stato istituito il Dipartimento Tecnico Patrimoniale di cui fa parte la UOC Sistemi E Tecnologie Informatiche e di Comunicazione;

RICHIAMATA la Deliberazione n. 179 del 27/02/2020, avente ad oggetto "Atto aziendale dell'ASL Roma 1, approvato con Deliberazione n. 1153 del 17/12/2019 – Presa d'atto dell'esito positivo del procedimento di verifica regionale – Attuazione del nuovo modello organizzativo" la quale prevede l'attivazione del sopra citato Dipartimento e delle UU.OO.CC. nello stesso ricomprese;

VISTA la Delibera n. 347 del 08/07/2022 avente ad oggetto "*Sistema aziendale di deleghe e conseguente individuazione delle competenze nell'adozione degli atti amministrativi*" con la quale, tra l'altro, sono state individuate le competenze nell'adozione degli atti amministrativi;

VISTO il D.LGS. 50 del 18 aprile 2016 "Codice dei contratti pubblici" e ss.mm. ii;

PREMESSO che con Delibera n. 683 del 28/09/2022 l'azienda ASL Roma 1 ha approvato il Documento Unico di Programmazione, comprendente il Programma biennale degli acquisti di beni e servizi (anni 2022-2024) ed il Programma triennale dei lavori (anni 2023-2025) dell'azienda medesima, ai sensi e per gli effetti dell'art. 21 D. Lgs. n. 50/2016 e ss.mm.ii;

che con Delibera n. 1250 del 29/12/2022 la Regione Lazio ha adottato il Piano biennale 2023-2024 degli acquisti di beni e servizi ai sensi dell'art. 498-ter del Regolamento regionale n. 1/2002 e ss.mm.ii;

che la ASL Roma 1 afferisce istituzionalmente al Servizio Sanitario Regionale ed opera, pertanto, all'interno delle linee di indirizzo normativo e di programmazione definite dalla Regione Lazio attraverso i suoi organi di governo e le articolazioni dell'amministrazione regionale;

che l'Azienda Sanitaria Locale, nel quadro delle risorse ad essa destinate, ha come scopo la promozione e la tutela della salute, sia individuale che collettiva, della popolazione residente e comunque presente a qualsiasi titolo nel proprio ambito

territoriale, per consentire la migliore qualità di vita possibile, garantendo ai cittadini i livelli essenziali di assistenza, definiti dal Servizio Sanitario Nazionale e Regionale, attraverso l'organizzazione e la gestione di servizi e prestazioni preventive, di cura e riabilitative, prodotte ed erogate nel rispetto dei principi di appropriatezza e sulla base delle più moderne conoscenze tecnico-scientifiche e in coerenza con le evidenze epidemiologiche assicurando, al contempo, i parametri qualitativi migliori come definiti dalle normative nazionali e internazionali e dagli indirizzi dell'Unione Europea, il rispetto degli obiettivi costituzionali nonché dei vincoli di bilancio definiti dalla programmazione nazionale e regionale;

che l'Azienda concorre, inoltre, alla realizzazione della più vasta missione del Servizio Sanitario della Regione Lazio, anche integrando i servizi sociali e socioassistenziali del Comune di Roma e dei Municipi di riferimento, per quanto espressamente previsto o delegato;

CONSIDERATO che l'Asl si pone l'obiettivo di rafforzare la postura, la governance e la maturità del modello organizzativo e tecnologico posto in essere per la Sicurezza informatica di tutto il Sistema informatico dell'Ente, ossia garantire Riservatezza, Integrità e Disponibilità del patrimonio informativo, con particolare riferimento ai dati personali, nel contesto del continuo processo di digitalizzazione dei servizi dell'ecosistema aziendale e delle evoluzioni delle reti sanitarie e verso le infrastrutture cloud;

che allo scopo di innovare i servizi ed incrementare la produttività dell'Amministrazione, la Sicurezza delle informazioni e la Privacy rappresentano gli elementi base abilitanti che consentono di raggiungere tale obiettivo con le dovute garanzie. In quest'ottica, l'eccellenza è il risultato che può essere raggiunto:

- migliorando quanto già in essere;
- innovando al fine di erogare e offrire nuovi servizi;
- attuando un adeguato processo di monitoraggio, misurazione e comunicazione della sicurezza delle informazioni;

che questo modello richiede e prevede l'adozione di un approccio di miglioramento continuo che consenta di rispondere alle mutate esigenze di contesto (normativo in primis), garantendo al contempo la continuità di quanto avviato;

CONSIDERATO ALTRESI'

che si rende necessario l'adozione di una visione strategica di lungo periodo e la definizione di piani tattici con risultati tangibili nel medio-breve periodo;

che occorre quindi che sia adottato un approccio «Business & Risk Based» che coniughi le attuali esigenze di business con specifiche logiche di rischio, quali:

- Nuove e più evolute esigenze dovute all'evoluzione del contesto;
- Esigenze di continuità operativa;
- Mutevoli Minacce esterne (es. rischi connaturati alla digitalizzazione, attacchi sempre più sofisticanti);

- Vincoli esterni (es. Regolamento Privacy Europeo («GDPR»), misure sicurezza AGID, Direttiva NIS, Direttive ENISA, ecc.);

che lo scenario normativo in cui il l'ASL opera, prevede la Normativa Europea, la Direttiva NIS, il Cyber Security Act ed il DL 105/2019 "Perimetro di sicurezza cibernetica" che sottolineano l'importanza dell'attenzione al fenomeno del cybercrime, il quale è in costante aumento anche nell'ambito PA;

che in tale contesto l'Ente si propone di attuare degli interventi finalizzati all'incremento complessivo e progressivo del livello di sicurezza dell'ASL e a contrastare il costante aumento delle minacce informatiche, anche in considerazione degli accadimenti che hanno avuto e hanno continui risvolti sulle PA italiane;

TENUTO CONTO

che la vigente normativa in materia di acquisizione beni e servizi, come da ultimo modificata dalla legge 28 dicembre 2015, n. 208, prevede l'obbligo per gli Enti del SSN:

- di approvvigionarsi utilizzando le convenzioni stipulate dalle centrali regionali di riferimento ovvero, qualora non siano operative convenzioni regionali, le convenzioni-quadro stipulate da Consip S.p.A.; (art. 1, comma 449, l. 296/2006; art. 1 comma 548, l. 208/2015);

ATTESTATO

che sul portale Acquistinretepa è presente l'Accordo Quadro avente ad oggetto "l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni – ID 2296", Lotto 2;

che l'Azienda intende avvalersi del predetto accordo quadro Consip e che pertanto ha presentato il proprio piano dei fabbisogni (All.1) in virtù del quale l'aggiudicataria RTI Deloitte Risk Advisory S.r.l. ha prodotto il Piano Operativo (ALL. 2), in cui nel dettaglio sono riportate le specifiche esigenze aziendali;

che il piano operativo presentato dal RTI risulta tecnicamente ed economicamente congruo a quanto richiesto dal piano dei fabbisogni aziendale;

che di seguito sono riportati i singoli servizi richiesti:

SERVIZI RICHIESTI				
ID	**NOME SERVIZIO**	**VOCE DI COSTO**	**QUANTITA'** (gg Team ottimale)	**IMPORTO (Esente IVA)**
Anno 2023				
L2.S16 – Security Strategy	Analisi della postura di cybersecurity e definizione del piano strategico di potenziamento relativamente ai **servizi IT centralizzati erogati dal Datacenter Principale di ASL Roma 1** (Ambito IT)	L2.S16 — gg/p Team ottimale	**480**	**120.000 €**
L2.S16 – Security Strategy	Cyber Security Awareness: 1) Estensione per 12 mesi dell'attuale progetto di Cyber Security Awareness supportato da relativa piattaforma; 2) Somministrazione di 4 corsi sulla norma ISO 27001	L2.S16 — gg/p Team ottimale	**672**	**168.000 €**

L2.S16 – Security Strategy	Cybersecurity Enforcement relativi alla Cloud Migration NOTA: Progetto attivabile da Luglio 2023	L2.S16 — gg/p Team ottimale	**400**	**100.000 €**
L2.S16 – Security Strategy	Mantenimento NIS e progressiva passaggio/estensione a NIS2	L2.S16 — gg/p Team ottimale	**500**	**125.000 €**
L2.S16 – Security Strategy	Progetto VAPT: Sviluppo evolutivo Portale "Security View"	L2.S16 — gg/p Team ottimale	**280**	**70.000 €**
L2.S22 – Penetration Test	Progetto VAPT: Attività di Vulnerability Assessment & Penetration Testing	L2.S22 – gg/p Team ottimale	**970**	**160.050 €**
Anno 2024				
L2.S16 – Security Strategy	Analisi della postura di cybersecurity e definizione del piano strategico di potenziamento relativamente **ai servizi IT afferenti a max 5 strutture territoriali di media/piccola complessità** (Ambito IT)	L2.S16 — gg/p Team ottimale	**600**	**150.000 €**
L2.S16 – Security Strategy	Cyber Security Awareness: 1) Estensione per 12 mesi dell'attuale progetto di Cyber Security Awareness supportato da relativa piattaforma; 2) Somministrazione di 5 sessioni formative relative a Perimetro Nazionale Sicurezza Cibernetico, NIS, NIS2, IS27001 (Overview) e formazione specialistica cyber	L2.S16 — gg/p Team ottimale	**688**	**172.000 €**
L2.S16 – Security Strategy	Cybersecurity Enforcement relativi alla Cloud Migration	L2.S16 — gg/p Team ottimale	**1120**	**280.000 €**
L2.S16 – Security Strategy	Mantenimento NIS e progressiva passaggio/estensione a NIS2	L2.S16 — gg/p Team ottimale	**500**	**125.000 €**
L2.S16 – Security Strategy	Progetto VAPT: Sviluppo evolutivo Portale "Security View"	L2.S16 — gg/p Team ottimale	**280**	**70.000 €**
L2.S22 – Penetration Test	Progetto VAPT: Attività di Vulnerability Assessment & Penetration Testing	L2.S22 – gg/p Team ottimale	**970**	**160.050 €**
Anno 2025				
L2.S16 – Security Strategy	Cybersecurity Enforcement relativi alla Cloud Migration	L2.S16 — gg/p Team ottimale	**1120**	**280.000 €**
L2.S16 – Security Strategy	Mantenimento NIS e progressiva passaggio/estensione a NIS2	L2.S16 — gg/p Team ottimale	**500**	**125.000 €**
L2.S22 – Penetration Test	Progetto VAPT: Attività di Vulnerability Assessment & Penetration Testing	L2.S22 – gg/p Team ottimale	**970**	**160.050 €**
			TOTALE (Esclusa IVA)	**2.265.150 €**

che l'Azienda provvederà pertanto, in conformità con quanto prescritto dall'accordo quadro a stipulare con l'Operatore Economico aggiudicatario un contratto esecutivo per la durata di mesi 36 mesi e per un importo complessivo di € 2.265.150 IVA esclusa, in conformità al piano operativo allegato;

DATO ATTO che, come previsto dalla normativa sulla tracciabilità dei flussi finanziari, di cui alla legge n. 136/2010, si è ottemperato alla generazione del CIG derivato 9668894FBA;

che, ai sensi del regolamento incentivi ex art. 113 del D.lgs. n. 50/2016 approvato con Delibera n. 13 del 19/04/2022, sono previste le seguenti quote per incentivi Funzioni tecniche, per un totale complessivo di € 7.177,70 così distribuito:

QUADRO ECONOMICO RIEPILOGATIVO	
a) Importo di affidamento	2.265.150,00 €
totale a)	**2.265.150,00 €**
b) SOMME A DISPOSIZIONE DELL'AMMINISTRAZIONE	
b1) incentivi ex art.113, **comma 3**, D.Lgs. n.50/2016	5.742,16 €
b2) incentivi ex art.113, **comma 4**, D.Lgs. n.50/2016	1.435,54 €
b3) IVA 22% su importo affidamento	498.333,00 €
totale b)	**505.510,69 €**
IMPORTO TOTALE a) + b)	**2.770.660,69 €**

Incentivi lordi per ruolo

Controllo esecuzione dei contratti pubblici	
b) Collaboratore/i RUP	883,41 €
c) Direttore dell'esecuzione*	3.533,63 €
d) Collaboratore /i DEC	1.325,11 €

che il costo complessivo derivante dal presente provvedimento, pari ad € 2.272.327,70 iva esclusa pari ad € 2.770.660,69 iva inclusa, comprensivo degli incentivi ex art. 113 Codice dei contratti, verrà imputato come segue:

- € 2.265.150, 00 Iva esclusa ovvero € 2.763.483,00 Iva inclusa, relativi all'adesione all'accordo quadro, sui conti di servizio come di seguito dettagliato:

  - € 906.521,00 Iva inclusa - CE 502020106 - Servizi di assistenza informatica – Bilancio 2023;

  - € 1.167.601,00 Iva inclusa - CE 502020106 - Servizi di assistenza informatica – Bilancio 2024.

- € 689.361,00 Iva inclusa - CE 502020106 - Servizi di assistenza informatica – Bilancio 2025.

- € 7.177,70 sul conto economico n. 516040605, rubricato "accantonamento incentivi funzioni tecniche art. 113 d.lgs. 50/2016", in applicazione delle percentuali e delle quote di ripartizione previste dal Regolamento aziendale a beneficio del/dei collaboratore/i del RUP, del DEC e collaboratori al DEC, che saranno successivamente liquidate con apposito provvedimento, secondo quanto stabilito all'art. 20 del Regolamento incentivi;

che si rinvia a successiva determinazione della struttura proponente il presente atto, ad esito della acquisizione della relazione del RUP sulla gestione della procedura di gara, la liquidazione delle spese dovute per la corresponsione dei suddetti incentivi, ai sensi dell'art. 113 d.lgs. 50/2016;

che a seguito dell'adozione del presente atto il CE 502020106 presenta la seguente situazione economica:

Budget assegnato	€ 17.116.518,00
Budget già impegnato	€ 11.655.019,80
Importo impegnato con il presente atto	€ 906.521,00
Residuo	€ 4.554.977,20

ATTESO che il Responsabile del Procedimento è il Direttore della U.O.C. Sistemi e Tecnologie Informatiche e di Comunicazione Ing. Debora Angeletti cui compete la verifica e l'accertamento della regolarità e qualità della fornitura resa, anche ai fini della liquidazione;

ATTESTATO che il presente provvedimento a seguito dell'istruttoria effettuata, nella forma e nella sostanza è totalmente legittimo, utile e proficuo per il servizio pubblico ai sensi e per gli effetti di quanto disposto dall'art. 1 della Legge n. 20/1994 e successive modifiche nonché alla stregua dei criteri di economicità e di efficacia di cui all'art. 1, comma 1, della Legge n. 241/1990 e successive modifiche ed integrazioni;

PROPONE

Per i motivi e le valutazioni sopra riportate, che formano parte integrante del presente atto:

di aderire all'Accordo Quadro Consip "Cybersecurity Enforcement- Lotto 2" (Cig madre 8884642E81) - SSN – ID 2296" con il Fornitore RTI Deloitte Risk Advisory S.r.l. (Mandataria), per la l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni per le esigenze della Asl Roma 1 - Importo complessivo pari ad pari ad € 2.271.223,44 iva esclusa, comprensivi delle quote per incentivi funzioni tecniche, €2.769.556,43 iva inclusa per un periodo di 36 mesi (CIG Derivato 9668894FBA);

di dare atto che la spesa derivante dal presente provvedimento, pari ad € 2.769.556,43 esclusa, comprensivo degli incentivi ex art. 113 Codice dei contratti, verrà imputata come segue:

- € 2.265.150, 00 Iva esclusa ovvero € 2.763.483,00 Iva inclusa, relativi all'adesione all'accordo quadro, sui conti di servizio come di seguito dettagliato:

  - € 906.521,00 Iva inclusa - CE 502020106 - Servizi di assistenza informatica – Bilancio 2023;

- € 1.167.601,00 Iva inclusa - CE 502020106 - Servizi di assistenza informatica – Bilancio 2024.

- € 689.361,00 Iva inclusa - CE 502020106 - Servizi di assistenza informatica – Bilancio 2025.

- € 7.177,70 sul conto economico n. 516040605, rubricato "accantonamento incentivi funzioni tecniche art. 113 d.lgs. 50/2016", in applicazione delle percentuali e delle quote di ripartizione previste dal Regolamento aziendale a beneficio del/dei collaboratore/i del RUP, del DEC e collaboratori al DEC, che saranno successivamente liquidate con apposito provvedimento, secondo quanto stabilito all'art. 20 del Regolamento incentivi;

e che si rinvia a successiva determinazione della struttura proponente il presente atto, ad esito della acquisizione della relazione del RUP sulla gestione della procedura di gara, la liquidazione delle spese dovute per la corresponsione dei suddetti incentivi, ai sensi dell'art. 113 d.lgs. 50/2016;

di nominare, ai sensi e per gli effetti dell'art. 101 del d.lgs. 50/2016, quale DEC per la procedura in oggetto, il Sig Stefano Scaramuzzino in qualità di referente tecnico NIS e assistente tecnico presso la UOC Sistemi e tecnologie informatiche e di comunicazione e come assistenti al DEC Sig. Luciano Marani, Dott.ssa Michela Mazzotta, Dott.ssa Francesca Caruso;

di incaricare il Dirigente proponente, ad avvenuta adozione della presente delibera, di predisporre tutti gli atti conseguenti e necessari per dare avvio al contenuto di cui al presente provvedimento, ivi comprese le relative notifiche e/o comunicazioni all'Operatore Economico interessato;

di disporre che il presente atto venga pubblicato in versione integrale nell'Albo Pretorio on line aziendale ai sensi dell'art. 32, comma 1, della legge 18.06.2009 n. 69, nel rispetto comunque della normativa sulla protezione dei dati personali e autorizzare il competente servizio aziendale ad oscurare eventuali dati non necessari rispetto alla finalità di pubblicazione.

Il Responsabile del procedimento	Il Direttore della U.O.C. Sistemi e Tecnologie Informatiche e di Comunicazione	Il Direttore Dipartimento Tecnico Patrimoniale
Ing. Debora Angeletti	Ing. Debora Angeletti	Ing. Paola Brazzoduro

IL DIRETTORE GENERALE F.F.

IN VIRTÚ dei poteri previsti:

- dall'art. 3 del D. Lgs 502/1992 e ss.mm.ii;
- dall'art. 8 della L.R. n. 18/1994 e ss.mm.ii;

nonché delle funzioni e dei poteri di cui alla Deliberazione del Direttore Generale n. 620 del 22/09/2022;

Letta la proposta di delibera sopra riportata presentata dal Dirigente Responsabile dell'Unità in frontespizio indicata;

PRESO ATTO che il Direttore della Struttura proponente il presente provvedimento, sottoscrivendolo, attesta che lo stesso, a seguito dell'istruttoria effettuata, nella forma e nella sostanza è totalmente legittimo, utile e proficuo per il servizio pubblico ai sensi e per gli effetti di quanto disposto dall'art. 1 della Legge n. 20/1994 e successive modifiche nonché alla stregua dei criteri di economicità e di efficacia di cui all'art. 1, comma 1, della Legge 241/1990 e successive modifiche ed integrazioni;

ACQUISITI i pareri favorevoli del Direttore Amministrativo e del Direttore Sanitario riportati in frontespizio;

DELIBERA

di adottare la proposta di deliberazione avente per oggetto " Adesione all'Accordo Quadro Consip "SERVIZI DI SICUREZZA DA REMOTO, COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI - Lotto 2" (Cig madre 8884642E81) - SSN – ID 2296" con il Fornitore RTI Deloitte Risk Advisory S.r.l. (Mandataria), per la l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni per le esigenze della Asl Roma 1 - Importo complessivo pari ad € 2.272.327,70 iva esclusa, comprensivi delle quote per incentivi funzioni tecniche (€ 2.770.660,69 iva inclusa) per un periodo di 36 mesi. (CIG Derivato 9668894FBA)" e conseguentemente, per i motivi e le valutazioni sopra riportate, che formano parte integrante del presente atto:

di aderire all'Accordo Quadro Consip "Cybersecurity Enforcement- Lotto 2" (Cig madre 8884642E81) - SSN – ID 2296" con il Fornitore RTI Deloitte Risk Advisory S.r.l. (Mandataria), per la l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni per le esigenze della Asl Roma 1 - Importo complessivo pari ad pari ad € 2.271.223,44 iva esclusa, comprensivi delle quote per incentivi funzioni tecniche, €2.769.556,43 iva inclusa per un periodo di 36 mesi (CIG Derivato 9668894FBA);

di dare atto che la spesa derivante dal presente provvedimento, pari ad € 2.769.556,43 esclusa, comprensivo degli incentivi ex art. 113 Codice dei contratti, verrà imputata come segue:

- € 2.265.150, 00 Iva esclusa ovvero € 2.763.483,00 Iva inclusa, relativi all'adesione all'accordo quadro, sui conti di servizio come di seguito dettagliato:

  - € 906.521,00 Iva inclusa - CE 502020106 - Servizi di assistenza informatica – Bilancio 2023;

  - € 1.167.601,00 Iva inclusa - CE 502020106 - Servizi di assistenza informatica – Bilancio 2024.

  - € 689.361,00 Iva inclusa - CE 502020106 - Servizi di assistenza informatica – Bilancio 2025.

- € 7.177,70 sul conto economico n. 516040605, rubricato "accantonamento incentivi funzioni tecniche art. 113 d.lgs. 50/2016", in applicazione delle percentuali e delle quote di ripartizione previste dal Regolamento aziendale a beneficio del/dei collaboratore/i del RUP, del DEC e collaboratori al DEC, che saranno successivamente liquidate con apposito provvedimento, secondo quanto stabilito all'art. 20 del Regolamento incentivi;

e che si rinvia a successiva determinazione della struttura proponente il presente atto, ad esito della acquisizione della relazione del RUP sulla gestione della procedura di gara, la liquidazione delle spese dovute per la corresponsione dei suddetti incentivi, ai sensi dell'art. 113 d.lgs. 50/2016;

di nominare, ai sensi e per gli effetti dell'art. 101 del d.lgs. 50/2016, quale DEC per la procedura in oggetto, il Sig Stefano Scaramuzzino in qualità di referente tecnico NIS e assistente tecnico presso la UOC Sistemi e tecnologie informatiche e di comunicazione e come assistenti al DEC Sig. Luciano Marani, Dott.ssa Michela Mazzotta, Dott.ssa Francesca Caruso;

di incaricare il Dirigente proponente, ad avvenuta adozione della presente delibera, di predisporre tutti gli atti conseguenti e necessari per dare avvio al contenuto di cui al presente provvedimento, ivi comprese le relative notifiche e/o comunicazioni all'Operatore Economico interessato;

di disporre che il presente atto venga pubblicato in versione integrale nell'Albo Pretorio on line aziendale ai sensi dell'art. 32, comma 1, della legge 18.06.2009 n. 69, nel rispetto comunque della normativa sulla protezione dei dati personali e autorizzare il competente servizio aziendale ad oscurare eventuali dati non necessari rispetto alla finalità di pubblicazione.

Il Responsabile della struttura proponente provvederà all'attuazione della presente deliberazione curandone altresì la relativa trasmissione agli uffici/organi rispettivamente interessati.

Il DIRETTORE GENERALE F.F.
Dr.ssa Roberta Volpini
FIRMATO DIGITALMENTE

Identificativo: Piano dei Fabbisogni – Cybersecurity Enforcement – ASL Roma 1

Data: 10/02/2023

ACCORDO QUADRO PER L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI

LOTTO 2 – SERVIZI DI COMPLIANCE E CONTROLLO

PUBBLICHE AMMINISTRAZIONI LOCALI

ASL Roma 1

Piano dei fabbisogni – Cybersecurity Enforcement

Costituito

Raggruppamento Temporaneo di Imprese

composto da:

Deloitte Risk Advisory S.r.l.

EY Advisory S.p.A.

Teleco S.r.l.

Deloitte. EY teleco

SOMMARIO

1 INTRODUZIONE

1.1 Ambito

Nel Settembre 2021 CONSIP ha bandito una procedura aperta, suddivisa in due lotti, per "l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni – ID 2296". Il Lotto 2, inerente ai servizi di compliance e controllo, è stato assegnato come primo aggiudicatario al Raggruppamento Temporaneo di Imprese (RTI), la cui mandataria è Deloitte Risk Advisory S.r.l. e le società mandanti sono EY Advisory S.p.A. e Teleco S.r.l., per la stipula di contratti esecutivi con le Pubbliche Amministrazioni Locali (PAL).

La durata dell'Accordo Quadro è di **24** mesi, decorrenti dalla data di attivazione. Per durata dell'Accordo Quadro si intende il periodo entro il quale le Amministrazioni potranno affidare, a seguito della approvazione del Piano Operativo, contratti esecutivi agli operatori economici aggiudicatari parti dell'Accordo Quadro per l'approvvigionamento dei servizi oggetto dell'Accordo Quadro. Ciascun Contratto esecutivo avrà una durata massima di 48 mesi decorrenti dalla relativa data di conclusione delle attività di presa in carico.

Il presente documento costituisce il "Piano dei fabbisogni" (o "Ordinativo di fornitura"), contenente i) i requisiti, i servizi, le caratteristiche qualitative, i dimensionamenti; ii) la descrizione del contesto tecnologico ed applicativo e la descrizione delle attività dimensionate, al fine di permettere la identificazione e contestualizzazione dei servizi nonché la eventuale declinazione delle figure professionali e degli strumenti a supporto.

1.2 Richieste dell'Amministrazione contraente

La ASL Roma 1 afferisce istituzionalmente al Servizio Sanitario Regionale ed opera, pertanto, all'interno delle linee di indirizzo normativo e di programmazione definite dalla Regione Lazio attraverso i suoi organi di governo e le articolazioni dell'amministrazione regionale.

L'Azienda Sanitaria Locale, nel quadro delle risorse ad essa destinate, ha come scopo la promozione e la tutela della salute, sia individuale che collettiva, della popolazione residente e comunque presente a qualsiasi titolo nel proprio ambito territoriale, per consentire la migliore qualità di vita possibile, garantendo ai cittadini i livelli essenziali di assistenza, definiti dal Servizio Sanitario Nazionale e Regionale, attraverso l'organizzazione e la gestione di servizi e prestazioni preventive, di cura e riabilitative, prodotte ed erogate nel rispetto dei principi di appropriatezza e sulla base delle più moderne conoscenze tecnico-scientifiche e in coerenza con le evidenze epidemiologiche assicurando, al contempo, i parametri qualitativi migliori come definiti dalle normative nazionali e internazionali e dagli indirizzi dell'Unione Europea, il rispetto degli obiettivi costituzionali nonché dei vincoli di bilancio definiti dalla programmazione nazionale e regionale.

L'Azienda concorre, inoltre, alla realizzazione della più vasta missione del Servizio Sanitario della Regione Lazio, anche integrando i servizi sociali e socioassistenziali del Comune di Roma e dei Municipi di riferimento, per quanto espressamente previsto o delegato.

In tale contesto, per l'ASL Roma 1, aumentare il know-how e la consapevolezza sui rischi inerenti alla propria organizzazione e ai propri servizi e infrastrutture informatiche riveste un'importanza centrale, così come programmare le azioni da attuare per mitigare i rischi e per contrastare eventi di cybercrime. Per tali ragioni, nell'ambito del contratto quadro per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni, l'Amministrazione ha richiesto, ai fini dello sviluppo del Progetto di Sicurezza, l'esecuzione dei servizi afferenti al Lotto 2- Servizi di Compliance e controllo:

1. ***L2.S16 – Servizio di Security Strategy****;*
2. ***L2.S22 – Penetration Testing.***

1.3 Riferimenti

IDENTIFICATIVO	TITOLO/DESCRIZIONE
ID 2296 – Gara Sicurezza da remoto – Allegato 1 – Capitolato Tecnico Generale	Capitolato Tecnico Generale della 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 – Gara Sicurezza da remoto – Allegato 2B – Capitolato Tecnico Speciale Lotto 2	Capitolato Tecnico Speciale della 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 – Gara Sicurezza da remoto – Capitolato Oneri	Capitolato d'Oneri della 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 – Gara Sicurezza da remoto – Bando GURI	Bando GURI della 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

1.4 Acronimi e glossario

DEFINIZIONE/ACRONIMO	DESCRIZIONE
RTI	Raggruppamento Temporaneo di Impresa
AQ	Accordo Quadro
ASL	Associazione Sanitaria Locale
CE	Contratto Esecutivo
PAL	Pubblica Amministrazione Locale

2 Anagrafica dell'amministrazione

DATI ANAGRAFICI DELL'AMMINISTRAZIONE	
Ragione sociale Amministrazione	[redacted]
Indirizzo	
CAP	
Comune	
Provincia	
Regione	
Codice Fiscale	
Indirizzo mail	
PEC	
Codice IPA	aslrm
Comparto di Appartenenza (PAL/PAC)	

DATI ANAGRAFICI REFERENTE DELL'AMMINISTRAZIONE	
Nome	[redacted]
[redacted]	[redacted]
Telefono	+[redacted]
[redacted]	[redacted]
PEC	

3 Contesto di riferimento

3.1 Contesto dei servizi

Il presente progetto si pone l'obiettivo di rafforzare la postura, la governance e la maturità del modello organizzativo e tecnologico posto in essere per la Sicurezza informatica di tutto il Sistema informatico dell'Ente, ossia garantire Riservatezza, Integrità e Disponibilità del patrimonio informativo, con particolare riferimento ai dati personali, nel contesto del continuo processo di digitalizzazione dei servizi dell'ecosistema aziendale e delle evoluzioni delle reti sanitarie e verso le infrastrutture cloud.

Allo scopo di innovare i servizi ed incrementare la produttività dell'Amministrazione, la Sicurezza delle informazioni e la Privacy rappresentano gli elementi base abilitanti che consentono di raggiungere tale obiettivo con le dovute garanzie. In quest'ottica, l'eccellenza è il risultato che può essere raggiunto:

- migliorando quanto già in essere;
- innovando al fine di erogare e offrire nuovi servizi;
- attuando un adeguato processo di monitoraggio, misurazione e comunicazione della sicurezza delle informazioni.

Questo modello richiede e prevede l'adozione di un approccio di miglioramento continuo che consenta di rispondere alle mutate esigenze di contesto (normativo in primis), garantendo al contempo la continuità di quanto avviato.

Inoltre, le sfide a cui si è chiamati a rispondere richiedono l'adozione di una visione strategica di lungo periodo e la definizione di piani tattici con risultati tangibili nel medio-breve periodo.

Occorre quindi che sia adottato un approccio «Business & Risk Based» che coniughi le attuali esigenze di business con specifiche logiche di rischio, quali:

- Nuove e più evolute esigenze dovute all'evoluzione del contesto,
- Esigenze di continuità operativa,
- Mutevoli Minacce esterne (es. rischi connaturati alla digitalizzazione, attacchi sempre più sofisticanti),
- Vincoli esterni (es. Regolamento Privacy Europeo («GDPR»), misure sicurezza AGID, Direttiva NIS, Direttive ENISA, ecc.).

Lo scenario normativo in cui il l'ASL opera prevede la Normativa Europea, la Direttiva NIS, il Cyber Security Act ed il DL 105/2019 "Perimetro di sicurezza cibernetica" che sottolineano l'importanza dell'attenzione al fenomeno del cybercrime, il quale è in costante aumento anche nell'ambito PA; fenomeno che è evidenziato come in crescita (Rapporto Clusit 2021) anche in relazione alle mutate condizioni lavorative dovute alla pandemia Covid.

In tale contesto l'Ente si propone di attuare degli interventi finalizzati all'incremento complessivo e progressivo del livello di sicurezza dell'ASL e a contrastare il costante aumento delle minacce informatiche, anche in considerazione degli accadimenti che hanno avuto e hanno continui risvolti sulle PA italiane.

3.2 Contesto tecnico ed operativo

Per tale fornitura non sono individuati specifici vincoli di tipo tecnico ed operativo tranne quelli legati al già dispiegato sistema di Cybersecurity aziendale di ASL Roma 1 che, grazie a questa fornitura, si implementerà delle necessarie componenti già citate in narrativa (cloud/normative etc.).

In termini di requisiti specifici per l'esecuzione delle attività oggetto dei servizi richiesti si rimanda ai requisiti trasversali previsti per l'Accordo Quadro.

La Unità Operativa Complessa (UOC) – Sistemi e Tecnologie informatiche e di comunicazione è il principale responsabile della sicurezza digitale in ASL Roma 1.

Si occupa prevalentemente della protezione dell'intera infrastruttura IT e dell'individuazione e della prevenzione delle minacce, implementando sistemi di sicurezza e misure di protezione e controllo.

Sebbene competenze e mansioni specifiche sono distribuite sia in ambito interno che in quello fornito da collaboratori esterni, è possibile stilare un elenco dei principali compiti che UOC STI svolge attualmente nel perimetro:

- La gestione dei sistemi aziendali di prevenzione;
- Il monitoraggio delle corrette esecuzioni delle best practices di sicurezza con la collaborazione del DPO interno ad ASL Roma 1;
- L'implementazione delle misure (quali firewall e sistemi di crittografia) che proteggono i dati aziendali e le informazioni sensibili;
- L'aggiornamento dei security tool utilizzati;
- L'individuazione delle intrusioni (i cosiddetti Data Breach) e attività non autorizzate;
- La raccolta delle informazioni sugli incidenti informatici isolando tutti parametri utili per prevedere e neutralizzare eventuali problematiche future;
- Lo studio delle security policy aziendali.

Le attività verranno condotte all'interno di eventuali gruppi di lavoro costituiti dagli interlocutori dell'Ente.y

3.3 Contesto Economico – Finanziario

Per l'attuazione delle attività di cui al presente Piano dei Fabbisogni è possibile da parte dell'Amministrazione il ricorso, in tutto o in parte, all'utilizzo dei fondi economici ai sensi del D.L. 77/2021.

4 Ambiti funzionali oggetto di intervento

Il profondo processo di trasformazione digitale avviato dall'Ente avente la finalità di portare innovazione nei servizi forniti, e la capacità di dover rispondere in maniera rapida ed efficace ai cambiamenti imposti anche dall'ambiente esterno pongono la necessità di non allentare mai l'attenzione alle tematiche che riguardano la sicurezza delle informazioni e la protezione dei dati.

Emergono di fatto nuove esigenze di sicurezza delle Informazioni e delle Infrastrutture dovute al mutamento degli scenari di rischio, dalle nuove minacce e dall'estensione delle superfici di attacco esposte, da un punto di vista sia interno (es. performance della modalità di lavoro remoto, gestione della sicurezza degli endpoint, miglioramento delle modalità di accesso da remoto ai sistemi) che esterno (es. evoluzioni di modalità e target degli attacchi).

Per il conseguimento di alcuni importanti obiettivi è richiesta l'attuazione delle seguenti principali azioni/macro attività:

- Analisi della postura di cybersecurity e definizione dei piani strategici di potenziamento in riferimento a diversi contesti e perimetri dell'ASL Roma 1;
- Attuazione di un processo di "Cybersecurity Enforcement" relativa alle attività di Cloud Migration di alcuni servizi IT erogati dall'ASL Roma 1;
- Mantenimento del sistema di conformità alla direttiva NIS e al progressivo passaggio/estensione alla versione NIS2;
- Verifica continuativa dei livelli di sicurezza di infrastrutture e applicazioni mediante attività di implementazione e potenziamento della attuale postura di Vulnerability Assessment e Penetration Testing.

4.1 Obiettivi e benefici da perseguire

Il Progetto di Sicurezza mira ad eseguire una valutazione del livello di maturità del sistema di gestione della sicurezza e della conformità normativa dell'Ente al fine di identificare le relative azioni necessarie per il rafforzamento delle capacità di difesa cyber.

Le azioni di rafforzamento, che saranno identificate all'interno de Piano Strategico e di Attuazione, potranno condurre all'adozione di nuovi presidi di sicurezza o portare ad un'estensione di quelli già esistenti, necessari al fine di fronteggiare in maniera più efficace i rischi cyber.

L'elaborazione e l'implementazione di un Piano Strategico aiuterà, altresì, l'Ente ad avere ben chiari gli obiettivi e a definire le linee guida per uniformare l'intero sistema di gestione della sicurezza ai principali framework nazionali e internazionali di cybersecurity e alle leggi e direttive vigenti (es: Direttiva NIS/NIS2). Quanto descritto verrà indirizzato mediante una serie di attività comprese nel macro-servizio **L2.S16 – Security Strategy** dell'Accordo Quadro Consip, Lotto2.

Ulteriori attività utili al rafforzamento delle difese agli attacchi cyber avverranno mediante una serie di azioni progettuali di verifica del sistema informativo di ASL Roma 1 che permettano di far emergere eventuali vulnerabilità e criticità che possano essere sfruttate da hacker e malintenzionati per perpetrare attacchi anche gravi nei confronti dell'Ente. Queste ultime attività sono comprese nel macro-servizio **L2.S22 – Penetration Testing** dell'Accordo Quadro.

4.2 Categorizzazione dell'intervento

4.2.1 Categorizzazione di I livello

	AMBITO I LIVELLO (LAYER)	OBIETTIVI PIANO TRIENNALE
	SERVIZI	Servizi al cittadino
		Servizi a imprese e professionisti
		Servizi interni alla propria PA
		Servizi verso altre PA
	DATI	Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese
		Aumentare la qualità dei dati e dei metadati
		Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati
	PIATTAFORME	Favorire l'evoluzione delle piattaforme esistenti per migliorare i servizi offerti a cittadini ed imprese semplificando l'azione amministrativa
		Aumentare il grado di adozione ed utilizzo delle piattaforme abilitanti esistenti da parte delle PA
		Incrementare e razionalizzare il numero di piattaforme per le amministrazioni al fine di semplificare i servizi ai cittadini
		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)
		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)
		Migliorare la fruizione dei servizi digitali per cittadini ed imprese tramite il potenziamento della connettività per le PA
	INTEROPERABILITÀ	Favorire l'applicazione della Linea guida sul Modello di Interoperabilità da parte degli erogatori di API
		Adottare API conformi al Modello di Interoperabilità
x	**SICUREZZA INFORMATICA**	Aumentare la consapevolezza del rischio cyber (Cyber Security Awareness) nelle PA
		Aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione

4.2.2 Categorizzazione di II livello

I LIVELLO (LAYER)		II LIVELLO
SERVIZI		Servizi al cittadino
		Servizi a imprese e professionisti
	X	Servizi interni alla propria PA

		Servizi verso altre PA
PIATTAFORME		Sanità digitale (FSE e CUP)
		Identità Digitale
		Pagamenti digitali
		App IO
		ANPR
		NoiPA
		INAD
		Musei
		Siope+
DATI		Agricoltura, pesca, silvicoltura e prodotti alimentari
		Economia e finanze
		Istruzione, cultura e sport
		Energia
		Ambiente
		Governo e Settore pubblico
	X	Salute
		Tematiche internazionali
		Giustizia e sicurezza pubblica
		Regioni e città
	X	Popolazione e società
		Scienza e tecnologia
		Trasporti
INTEROPERABILITA		Agricoltura, pesca, silvicoltura e prodotti alimentari
		Economia e finanze
		Istruzione, cultura e sport
		Energia
		Ambiente
		Governo e Settore pubblico
	X	Salute
		Tematiche internazionali
		Giustizia e sicurezza pubblica
		Regioni e città
		Popolazione e società
	X	Scienza e tecnologia
		Trasporti
INFRASTRUTTURE	X	Data center e Cloud
	x	Connettività
SICUREZZA INFORMATICA	X	Portali istituzionali e CMS
	X	Sensibilizzazione del rischio cyber

5 Servizi richiesti

SERVIZI RICHIESTI				
ID	**NOME SERVIZIO**	**VOCE DI COSTO**	**QUANTITA'** (gg Team ottimale)	**IMPORTO** (Esente IVA)
Anno 2023				
L2.S16 – Security Strategy	Analisi della postura di cybersecurity e definizione del piano strategico di potenziamento relativamente ai **servizi IT centralizzati erogati dal Datacenter Principale di ASL Roma 1** (Ambito IT)	L2.S16 — gg/p Team ottimale	**480**	**120.000 €**
L2.S16 – Security Strategy	Cyber Security Awareness: 1) Estensione per 12 mesi dell'attuale progetto di Cyber Security Awareness supportato da relativa piattaforma; 2) Somministrazione di 4 corsi sulla norma ISO 27001	L2.S16 — gg/p Team ottimale	**672**	**168.000 €**
L2.S16 – Security Strategy	Cybersecurity Enforcement relativi alla Cloud Migration NOTA: Progetto attivabile da Luglio 2023	L2.S16 — gg/p Team ottimale	**400**	**100.000 €**
L2.S16 – Security Strategy	Mantenimento NIS e progressiva passaggio/estensione a NIS2	L2.S16 — gg/p Team ottimale	**500**	**125.000 €**
L2.S16 – Security Strategy	Progetto VAPT: Sviluppo evolutivo Portale "Security View"	L2.S16 — gg/p Team ottimale	**280**	**70.000 €**
L2.S22 – Penetration Test	Progetto VAPT: Attività di Vulnerability Assessment & Penetration Testing	L2.S22 – gg/p Team ottimale	**970**	**160.050 €**
Anno 2024				
L2.S16 – Security Strategy	Analisi della postura di cybersecurity e definizione del piano strategico di potenziamento relativamente **ai servizi IT afferenti a max 5 strutture territoriali di media/piccola complessità** (Ambito IT)	L2.S16 — gg/p Team ottimale	**600**	**150.000 €**
L2.S16 – Security Strategy	Cyber Security Awareness: 1) Estensione per 12 mesi dell'attuale progetto di Cyber Security Awareness supportato da relativa piattaforma; 2) Somministrazione di 5 sessioni formative relative a Perimetro Nazionale Sicurezza Cibernetico, NIS, NIS2, IS27001 (Overview) e formazione specialistica cyber	L2.S16 — gg/p Team ottimale	**688**	**172.000 €**
L2.S16 – Security Strategy	Cybersecurity Enforcement relativi alla Cloud Migration	L2.S16 — gg/p Team ottimale	**1120**	**280.000 €**

L2.S16 – Security Strategy	Mantenimento NIS e progressiva passaggio/estensione a NIS2	L2.S16 — gg/p Team ottimale	**500**	**125.000 €**
L2.S16 – Security Strategy	Progetto VAPT: Sviluppo evolutivo Portale "Security View"	L2.S16 — gg/p Team ottimale	**280**	**70.000 €**
L2.S22 – Penetration Test	Progetto VAPT: Attività di Vulnerability Assessment & Penetration Testing	L2.S22 – gg/p Team ottimale	**970**	**160.050 €**
Anno 2025				
L2.S16 – Security Strategy	Cybersecurity Enforcement relativi alla Cloud Migration	L2.S16 — gg/p Team ottimale	**1120**	**280.000 €**
L2.S16 – Security Strategy	Mantenimento NIS e progressiva passaggio/estensione a NIS2	L2.S16 — gg/p Team ottimale	**500**	**125.000 €**
L2.S22 – Penetration Test	Progetto VAPT: Attività di Vulnerability Assessment & Penetration Testing	L2.S22 – gg/p Team ottimale	**970**	**160.050 €**
			TOTALE (Esclusa IVA)	**2.265.150 €**

5.1 Dettaglio dei servizi richiesti

5.1.1 L2.S16 – Security Strategy

5.1.1.1 Descrizione e caratteristiche del servizio

Anni	Macro-attività	Attività	Deliverable
2023 – 2024 – 2025	**Analisi della postura di cybersecurity e definizione del piano strategico di potenziamento (Ambito IT)**	Esecuzione di una serie di **Assessment di Sicurezza** erogati nei confronti di **diversi contesti e perimetri**, finalizzati all'analisi dei livelli di maturità delle capacità cyber in termini di organizzazione, processi e tecnologie (People, Process & Technology) e successiva identificazione delle principali iniziative che costituiranno i piani strategici dell'Ente in riferimento ai diversi contesti e perimetri, secondo programmi pluriennale e con azioni di rimedio a breve-medio-lungo termine. In termini di perimetri, si sono identificati i seguenti: 1) Servizi IT centralizzati ed erogati dal Datacenter Principali (San Filippo Neri). Nota: verrà considerato un perimetro di analisi che comprenda l'erogazione di un campione di massimo 50 servizi IT che possano considerarsi rappresentativi in termini di complessità e criticità (es: Posta elettronica, File sharing, servizi amministrativi e contabili, ecc); 2) Assessment sui servizi IT afferenti a max 5 strutture territoriali di media/piccola complessità (es: Ospedale Santo Spirito, Ospedale Oftalmico, Santa Maria della Pietà, ecc). Analisi di alto livello sui servizi IT afferenti a max 5 strutture territoriali di media/piccola complessità. Nota: per ogni struttura territoriale verrà considerato un perimetro di analisi che comprenda l'erogazione di un campione di massimo 20 servizi IT che possano considerarsi rappresentativi in termini di complessità e criticità.	• Risultati dell'Assessment (Executive Summary e Detail Report) • Piani Strategici di Sicurezza a breve, medio e lungo termine (Executive Summary e Detail Report)
2023	**Cyber Security Awareness**	1) Progetto di Cyber Security Awareness supportato dalla relativa piattaforma; 2) Somministrazione di 4 corsi sulla norma ISO 27001 (max 10 persone, durata 5 gg) comprensivi di rilascio di attestati di frequenza, esame e certificazione	• Materiale formativo del corso • Attestato di frequenza e certificazione

2024	**Cyber Security Awareness**	1) Progetto di Cyber Security Awareness supportato dalla relativa piattaforma; 3) Somministrazione di 5 sessioni formative (max 10 persone, durata 3 gg) relativi a Perimetro Nazionale Sicurezza Cibernetico, NIS, NIS2, IS27001 (Overview) e formazione specialistica cyber su personale di UOC con rilascio di attestati di frequenza	• Materiale formativo del corso • Attestati di frequenza
2023 (da Settembre) – 2024 – 2025	**Cybersecurity Enforcement relativo alla Cloud Migration**	Servizio di affiancamento alle attività di Cloud Migration (IaaS/PaaS) che ASLR1 sta per intraprendere. Il supporto consiste in analisi puntuale dei requisiti di Cybersecurity di ASLR1 e la definizione dell'organizzazione, dei processi e delle tecnologie di Cloud Security che sarà necessario garantire e predisporre nella migrazione al Cloud per assicurare gli adeguati livelli di Riservatezza, Integrità, Disponibilità e Conformità di dati e servizi migrati nel Cloud. Nel dettaglio i servizi inclusi sono: 1) **Cloud Security Control Library**: Definizione di una libreria di controlli di sicurezza tecnici e organizzativi per gli ambienti cloud che considera i domini application, data, identity, infrastructure, monitoring, response e strategy & governance; 2) **Cloud Security Architecture**: disegno di una Security blueprint architetturale partendo dalle capability di sicurezza attualmente presenti nel contesto onprem, riviste in un'ottica Cloud, e valutando eventuali funzionalità offerte dal CSP al fine di complementare le misure di sicurezza minime necessarie; 3) **Cloud Security Governance framework**: sviluppo di linee guida di security e compliance per l'adozione e l'implementazione sicura dei servizi cloud, e revisione dei principali processi di security in ottica cloud. Il servizio prevede la revisione di 6 processi di gov già esistenti oppure la definizione ex-novo di 3 processi (es: Change Management, Cyber Incident Management, Accesso Control & User Access Management, ecc) 4) **Supporto nella verifica delle configurazioni sicura dell'ambiente Cloud** mediante assessment periodici di Posture Management al fine di governare eventuali misconfiguration lungo la migrazione dei servizi in Cloud NOTA: I servizi elencati sono stati stimati e si riferiscono a: - migrazione dei servizi verso 1 CSP Pubblico (es: AWS, Azure o GCP). Tali valori potrebbero essere rivisti al rialzo nel caso di migrazioni verso CSP diversi da quelli indicati; - un numero massimo di 500 oggetti migrati in Cloud.	• Libreria controlli • 1 Architettura Cloud Sicura • Cloud Security Governance Framework • Cloud Security Posture (2 report mensili) per 12 mesi

2023 – 2024 – 2025	**Mantenimento NIS e progressiva passaggio/estensione a NIS2**	Serie di servizi di indirizzo per la conformità alla NIS e di supporto per il passaggio graduale e all'estensione alla NIS2. I servizi comprendono: 1) Supporto al monitoraggio e reporting (PMO) del remediation plan NIS; 2) Supporto alla revisione/aggiornamento di policy/procedure Cyber per indirizzare i gap; 3) Monitoraggio degli sviluppi normativi in ambito NIS2; 4) Supporto all'analisi delle implicazioni per ASL Roma 1 derivanti dalla NIS2. NOTE: - Si assume che sia già stato effettuato negli anni scorsi un risk/maturity assessment rispetto alle linee guida NIS ministeriali e che sia già disponibile il piano di remediation con gli interventi da implementare. Non è previsto un re-assessment rispetto alle misure, eventualmente indirizzabile con collaborazione specifica; - Non sono previste attività di implementazione di soluzioni/tecnologie, eventualmente indirizzabili con collaborazione specifica; - Le attività di revisione/aggiornamento delle policy/procedure Cyber a di ASL Roma 1 saranno valutate volta per volta, compatibilmente con le attività di PMO in cui il team del fornitore è impegnato. Qualora l'effort richiesto al fornitore non fosse compatibile con le attività di PMO pattuite, le nuove attività potranno essere indirizzate con collaborazione specifica; - Con riferimento alla NIS2, il fornitore fornisce un supporto interpretativo prettamente tecnico, eventuale supporto di natura legale può essere indirizzabile con collaborazione specifica.	• Presentazioni di SAL e reporting executive periodici sullo stato avanzamento del remediation plan • Presentazioni sulla nuova normativa NIS2
2023 – 2024	**Progetto VAPT – Sviluppo evolutivo Portale "Security View "**	Progetto di sviluppo evolutivo ad-hoc sul portale Security View di un servizio di importazione di bollettini di sicurezza provenienti da fonti esterne pubbliche e private con, in particolare, la ricezione periodica delle informative provenienti dalla Polizia dello Stato in un formato testuale concordato e che andranno ad alimentare eventuali azioni di VA e PT. Parallelamente le stesse attività di scansione periodica possono generare notifiche esportabili verso sistemi terzi con lo scopo di alimentare una libreria comune di vulnerabilità in ambito applicativo sanitario. L'attività di import/export di security bullettin sarà possibile direttamente da interfaccia web oltre alla visualizzazione, ricerca e gestione dei dati.	• Import e visualizzazione in dashboard di bollettini di sicurezza • Export, in formato concordato, di un sottoinsieme dei risultati di VA e PT su applicativi sanitari

5.1.1.2 Modalità di erogazione e consuntivazione

Coerentemente a quanto previsto nel "CAPITOLATO TECNICO SPECIALE SERVIZI DI COMPLIANCE E CONTROLLO" si precisa che la modalità di remunerazione di tali servizi è "progettuale (a corpo)" e che la metrica di misurazione è "*giorni/persona del team ottimale*".

Saranno definiti di concerto con l'Amministrazione dei task e dei deliverable, dimensionati e valorizzati economicamente. La consuntivazione avverrà sulla base dello stato dell'avanzamento lavori mensile e dei deliverable approvati e consegnati determinato coerentemente con il piano di lavoro definito.

Il team di lavoro per la realizzazione delle attività sopraccitate prevede il coinvolgimento delle seguenti figure professionali:

- Security Principal
- Security Solution Architect
- Senior Information Security Consultant
- Senior Security Auditor
- Data Protection Specialist

Le attività potranno essere erogate presso varie sedi di Roma dell'Amministrazione Contraente o da remoto presso le sedi del RTI.

5.1.1.3 Attivazione e durata

Si prevede l'avvio del servizio entro il Q1 2023 per una durata di 36 mesi.

5.1.2 L2.S22 – Penetration Test

5.1.2.1 Descrizione e caratteristiche del servizio

Anni	Macro-attività	Attività	Deliverable
2023 – 2024 – 2025	**Progetto VAPT – Vulnerability Assessment e Penetration Testing**	Progetto di Vulnerability Assessment (VA) che prevede la procedura di enumerazione servizi esposti per ogni IP e per ogni FQDN oggetto di Assessment, e ricerca delle vulnerabilità note per ogni servizio rilevato. Il progetto prevede: 1) un piano di "Scanning" mensile da Internet su sistemi esterni (Data Center e Cloud); 2) un piano di "Scanning" semestrale da rete locale su sistemi interni (fino a 20 IP a campione). 3) esecuzione in modalità "on-demand" di simulazioni dei tentativi di accesso ai sistemi/servizi/applicazioni "Penetration Test" (PT), sfruttando le vulnerabilità rilevate nella fase precedente di VA, sui servizi che si decide di approfondire. I risultati delle attività di VA e PT potranno essere esposti attraverso il portale di sicurezza denominato "Security View". Nel progetto vengo incluse anche alcune attività relative alla soluzione già in uso presso ASL, di Mail Security di frontiera LibraEsva. Tali attività permetteranno la raccolta e l'indicizzazione dei log collezionati dalla piattaforma che verranno poi organizzate in opportuni report utili ad evidenziare vulnerabilità ed anomalie potenzialmente critiche (es: tentativi non autorizzati di accesso, traffico anomalo, attacchi virali o violazione delle policy) e identificare gli IOC (Indicator Of Compromise) e per estensione anche gli IOA (Indicator Of Attack).	• Vulnerability Report: vulnerabilità per ogni singolo host con relativo trend basato sulla storicizzazione degli scan effettuati. • Remediation Plan: viene presentato il piano di azioni da percorrere per la messa in sicurezza delle vulnerabilità rilevate. • Mail Security Report utili ad evidenziare vulnerabilità ed anomalie potenzialmente critiche e IOC/IOA

5.1.2.2 Modalità di erogazione e consuntivazione

Coerentemente a quanto previsto nel "CAPITOLATO TECNICO SPECIALE SERVIZI DI COMPLIANCE E CONTROLLO" si precisa che la modalità di remunerazione di tali servizi è "progettuale (a corpo)" e che la metrica di misurazione è "*giorni/persona*".

Saranno definiti di concerto con l'Amministrazione dei task e dei deliverable, dimensionati e valorizzati economicamente. La consuntivazione avverrà sulla base dello stato dell'avanzamento lavori mensile e dei deliverable approvati e consegnati determinato coerentemente con il piano di lavoro definito.

Il team di lavoro per la realizzazione delle attività sopraccitate prevede il coinvolgimento delle seguenti figure professionali:

- Security Principal

- Senior Penetration tester
- Junior Penetration tester
- Forensic Expert

Le attività potranno essere erogate presso varie sedi di Roma dell'Amministrazione Contraente o da remoto presso le sedi del RTI.

5.1.2.3 Attivazione e durata

Si prevede l'avvio del servizio entro Q1 2023 per una durata di 36 mesi.

5.2 Organizzazione e figure di riferimento dell'amministrazione

I principali punti di contatto tecnici dell'amministrazione per l'esecuzione del presente progetto sono il Direttore UOC Sistemi e tecnologie informatiche e di comunicazione, il Responsabile della transizione digitale, il Referente NIS e il Referente tecnico NIS.

L'amministrazione si riserva di poter identificare durante l'esecuzione del contratto ulteriori figure di riferimento con le quali il fornitore potrà interfacciarsi.

5.3 Organizzazione e figure di riferimento del fornitore

Si richiede di indicare nel Piano Operativo le persone incaricate dal Fornitore per la conduzione del progetto e i relativi ruoli/responsabilità.

6 Elementi quantitativi e qualitativi per il dimensionamento servizi

6.1 Elementi quantitativi dei servizi

Si riporta di seguito una caratterizzazione quantitativa di riferimento data dalla complessità dei progetti individuati:

ID	NOME SERVIZIO	Gg/p Team ottimale	Uffici interessati	Ambiti di servizio	Numero Key user coinvolti	Numero Volumi
Anno 2023						
L2.S16	Security Strategy	**2.332**	N/D	> 40	< 20	N/A
L2.S22	Penetration Test	**970**	N/D	> 40	< 20	N/A
Anno 2024						
L2.S16	Security Strategy	**3.188**	N/D	> 40	< 20	N/A
L2.S22	Penetration Test	**970**	N/D	> 40	< 20	N/A
Anno 2025						
L2.S16	Security Strategy	**1.620**	N/D	> 40	< 20	N/A
L2.S22	Penetration Test	**970**	N/D	> 40	< 20	N/A

6.2 Elementi qualitativi dei servizi

I servizi dovranno essere svolti tenendo conto delle linee guida tecniche e la normativa vigente o le successive modifiche che verranno individuate.

6.3 Pianificazione dei servizi

La durata ipotizzata per la fornitura è di 36 mesi dalla data di attivazione, compatibilmente con il vincolo definito dall'Accordo Quadro, ovvero che i Contratti Esecutivi hanno una durata massima pari alla durata residua, al momento della sua stipula, dell'Accordo Quadro.

Di seguito si riporta la pianificazione di massima del programma con indicazione degli obiettivi in ambito del presente piano dei fabbisogni.

Obiettivi/Servizi	Anno 2023				Anno 2024				Anno 2025			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
L2.S16												
L2.S22												

Identificativo: Piano Operativo – Servizi di gestione incidenti e strumenti di supporto – ASL Roma 1

Data: 15/02/2023

ACCORDO QUADRO PER L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI

LOTTO 2 – SERVIZI DI COMPLIANCE E CONTROLLO

PUBBLICHE AMMINISTRAZIONI LOCALI

Piano Operativo – Servizi di gestione incidenti e strumenti di supporto

ASL Roma1

Costituito

Raggruppamento Temporaneo di Imprese

composto da:

Deloitte Risk Advisory S.r.l.

EY Advisory S.p.A.

Teleco S.r.l.

Deloitte. EY teleco

1 INTRODUZIONE

1.1 Ambito

Nel Settembre 2021 CONSIP ha bandito una procedura aperta, suddivisa in due lotti, per "l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni – ID 2296". Il Lotto 2, inerente ai servizi di compliance e controllo, è stato assegnato come primo aggiudicatario al Raggruppamento Temporaneo di Imprese (RTI), la cui mandataria è Deloitte Risk Advisory S.r.l. e le società mandanti sono EY Advisory S.p.A. e Teleco S.r.l., per la stipula di contratti esecutivi con le Pubbliche Amministrazioni Locali (PAL).

La durata dell'Accordo Quadro è di **24** mesi, decorrenti dalla data di attivazione. Per durata dell'Accordo Quadro si intende il periodo entro il quale le Amministrazioni potranno affidare, a seguito della approvazione del Piano Operativo, contratti esecutivi agli operatori economici aggiudicatari parti dell'Accordo Quadro per l'approvvigionamento dei servizi oggetto dell'Accordo Quadro. Ciascun Contratto esecutivo avrà una durata massima di 48 mesi decorrenti dalla relativa data di conclusione delle attività di presa in carico.

Il presente documento costituisce il "Piano dei fabbisogni" (o "Ordinativo di fornitura"), contenente i) i requisiti, i servizi, le caratteristiche qualitative, i dimensionamenti; ii) la descrizione del contesto tecnologico ed applicativo e la descrizione delle attività dimensionate, al fine di permettere la identificazione e contestualizzazione dei servizi nonché la eventuale declinazione delle figure professionali e degli strumenti a supporto.

1.2 Richieste dell'Amministrazione contraente

La ASL Roma 1 afferisce istituzionalmente al Servizio Sanitario Regionale ed opera, pertanto, all'interno delle linee di indirizzo normativo e di programmazione definite dalla Regione Lazio attraverso i suoi organi di governo e le articolazioni dell'amministrazione regionale.

L'Azienda Sanitaria Locale, nel quadro delle risorse ad essa destinate, ha come scopo la promozione e la tutela della salute, sia individuale che collettiva, della popolazione residente e comunque presente a qualsiasi titolo nel proprio ambito territoriale, per consentire la migliore qualità di vita possibile, garantendo ai cittadini i livelli essenziali di assistenza, definiti dal Servizio Sanitario Nazionale e Regionale, attraverso l'organizzazione e la gestione di servizi e prestazioni preventive, di cura e riabilitative, prodotte ed erogate nel rispetto dei principi di appropriatezza e sulla base delle più moderne conoscenze tecnico-scientifiche e in coerenza con le evidenze epidemiologiche assicurando, al contempo, i parametri qualitativi migliori come definiti dalle normative nazionali e internazionali e dagli indirizzi dell'Unione Europea, il rispetto degli obiettivi costituzionali nonché dei vincoli di bilancio definiti dalla programmazione nazionale e regionale.

L'Azienda concorre, inoltre, alla realizzazione della più vasta missione del Servizio Sanitario della Regione Lazio, anche integrando i servizi sociali e socioassistenziali del Comune di Roma e dei Municipi di riferimento, per quanto espressamente previsto o delegato.

In tale contesto, per l'ASL Roma 1, aumentare il know-how e la consapevolezza sui rischi inerenti alla propria organizzazione e ai propri servizi e infrastrutture informatiche riveste un'importanza centrale, così come programmare le azioni da attuare per mitigare i rischi e per contrastare eventi di cybercrime. Per tali ragioni, nell'ambito del contratto quadro per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni, l'Amministrazione ha richiesto, ai fini dello sviluppo del Progetto di Sicurezza, l'esecuzione dei servizi afferenti al Lotto 2- Servizi di Compliance e controllo:

1. ***L2.S16 – Servizio di Security Strategy****;*
2. ***L2.S22 – Penetration Testing.***

1.3 Riferimenti

IDENTIFICATIVO	TITOLO/DESCRIZIONE
ID 2296 - Gara Sicurezza da remoto - Allegato 1 - Capitolato Tecnico Generale	Capitolato Tecnico Generale della 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 - Gara Sicurezza da remoto - Allegato 2B - Capitolato Tecnico Speciale Lotto 2	Capitolato Tecnico Speciale della 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 - Gara Sicurezza da remoto - Capitolato Oneri	Capitolato d'Oneri della 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 - Gara Sicurezza da remoto - Bando GURI	Bando GURI della 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

1.4 Acronimi e glossario

DEFINIZIONE/ACRONIMO	DESCRIZIONE
RTI	Raggruppamento Temporaneo di Impresa
AQ	Accordo Quadro
ASL	Associazione Sanitaria Locale
CE	Contratto Esecutivo
PAL	Pubblica Amministrazione Locale

2 Anagrafica dell'amministrazione

DATI ANAGRAFICI DELL'AMMINISTRAZIONE	
Ragione sociale Amministrazione	[redacted]
Indirizzo	
CAP	
Comune	
Provincia	
Regione	
Codice Fiscale	
Indirizzo mail	
PEC	
Codice IPA	
Comparto di Appartenenza (PAL/PAC)	

DATI ANAGRAFICI REFERENTE DELL'AMMINISTRAZIONE	
Nome	[redacted]
Cognome	
Telefono	
Indirizzo mail	
PEC	

3 CATEGORIZZAZIONE DELL'INTERVENTO

3.1 Categorizzazione di I livello

	AMBITO I LIVELLO (LAYER)	OBIETTIVI PIANO TRIENNALE
	SERVIZI	Servizi al cittadino
		Servizi a imprese e professionisti
		Servizi interni alla propria PA
		Servizi verso altre PA
	DATI	Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese
		Aumentare la qualità dei dati e dei metadati
		Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati
	PIATTAFORME	Favorire l'evoluzione delle piattaforme esistenti per migliorare i servizi offerti a cittadini ed imprese semplificando l'azione amministrativa
		Aumentare il grado di adozione ed utilizzo delle piattaforme abilitanti esistenti da parte delle PA
		Incrementare e razionalizzare il numero di piattaforme per le amministrazioni al fine di semplificare i servizi ai cittadini
		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)
		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)
		Migliorare la fruizione dei servizi digitali per cittadini ed imprese tramite il potenziamento della connettività per le PA
	INTEROPERABILITÀ	Favorire l'applicazione della Linea guida sul Modello di Interoperabilità da parte degli erogatori di API
		Adottare API conformi al Modello di Interoperabilità
X	SICUREZZA INFORMATICA	Aumentare la consapevolezza del rischio cyber (Cyber Security Awareness) nelle PA
		Aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione

3.2 Categorizzazione di II livello

I LIVELLO (LAYER)		II LIVELLO
SERVIZI		Servizi al cittadino
		Servizi a imprese e professionisti
		Servizi interni alla propria PA
		Servizi verso altre PA

PIATTAFORME		Sanità digitale (FSE e CUP)
		Identità Digitale
		Pagamenti digitali
		App IO
		ANPR
		NoiPA
		INAD
		Musei
		Siope+
DATI		Agricoltura, pesca, silvicoltura e prodotti alimentari
		Economia e finanze
		Istruzione, cultura e sport
		Energia
		Ambiente
		Governo e Settore pubblico
		Salute
		Tematiche internazionali
		Giustizia e sicurezza pubblica
		Regioni e città
		Popolazione e società
		Scienza e tecnologia
		Trasporti
INTEROPERABILITA		Agricoltura, pesca, silvicoltura e prodotti alimentari
		Economia e finanze
		Istruzione, cultura e sport
		Energia
		Ambiente
		Governo e Settore pubblico
		Salute
		Tematiche internazionali
		Giustizia e sicurezza pubblica
		Regioni e città
		Popolazione e società
		Scienza e tecnologia
		Trasporti
INFRASTRUTTURE		Data center e Cloud
		Connettività
SICUREZZA INFORMATICA	**X**	Portali istituzionali e CMS
	X	Sensibilizzazione del rischio cyber

4 Servizi richiesti e ambito di intervento

4.1 Ambiti di intervento

Il profondo processo di trasformazione digitale avviato dall'Ente avente la finalità di portare innovazione nei servizi forniti, e la capacità di dover rispondere in maniera rapida ed efficace ai cambiamenti imposti anche dall'ambiente esterno pongono la necessità di non allentare mai l'attenzione alle tematiche che riguardano la sicurezza delle informazioni e la protezione dei dati.

Emergono di fatto nuove esigenze di sicurezza delle Informazioni e delle Infrastrutture dovute al mutamento degli scenari di rischio, dalle nuove minacce e dall'estensione delle superfici di attacco esposte, da un punto di vista sia interno (es. performance della modalità di lavoro remoto, gestione della sicurezza degli endpoint, miglioramento delle modalità di accesso da remoto ai sistemi) che esterno (es. evoluzioni di modalità e target degli attacchi).

Per il conseguimento di alcuni importanti obiettivi è richiesta l'attuazione delle seguenti principali azioni/macro attività:

- Analisi della postura di cybersecurity e definizione dei piani strategici di potenziamento in riferimento a diversi contesti e perimetri dell'ASL Roma 1;
- Attuazione di un processo di "Cybersecurity Enforcement" relativa alle attività di Cloud Migration di alcuni servizi IT erogati dall'ASL Roma 1;
- Mantenimento del sistema di conformità alla direttiva NIS e al progressivo passaggio/estensione alla versione NIS2;
- Verifica continuativa dei livelli di sicurezza di infrastrutture e applicazioni mediante attività di implementazione e potenziamento della attuale postura di Vulnerability Assessment e Penetration Testing.

Il Progetto di Sicurezza mira ad eseguire una valutazione del livello di maturità del sistema di gestione della sicurezza e della conformità normativa dell'Ente al fine di identificare le relative azioni necessarie per il rafforzamento delle capacità di difesa cyber.

Le azioni di rafforzamento, che saranno identificate all'interno de Piano Strategico e di Attuazione, potranno condurre all'adozione di nuovi presidi di sicurezza o portare ad un'estensione di quelli già esistenti, necessari al fine di fronteggiare in maniera più efficace i rischi cyber.

L'elaborazione e l'implementazione di un Piano Strategico aiuterà, altresì, l'Ente ad avere ben chiari gli obiettivi e a definire le linee guida per uniformare l'intero sistema di gestione della sicurezza ai principali framework nazionali e internazionali di cybersecurity e alle leggi e direttive vigenti (es: Direttiva NIS/NIS2). Quanto descritto verrà indirizzato mediante una serie di attività comprese nel macro-servizio **L2.S16 – Security Strategy** dell'Accordo Quadro Consip, Lotto2.

Ulteriori attività utili al rafforzamento delle difese agli attacchi cyber avverranno mediante una serie di azioni progettuali di verifica del sistema informativo di ASL Roma 1 che permettano di far emergere eventuali vulnerabilità e criticità che possano essere sfruttate da hacker e malintenzionati per perpetrare attacchi anche gravi nei confronti dell'Ente. Queste ultime attività sono comprese nel macro-servizio **L2.S22 – Penetration Testing** dell'Accordo Quadro.

4.2 Servizi richiesti

SERVIZI RICHIESTI				
ID	**NOME SERVIZIO**	**VOCE DI COSTO**	**QUANTITA'** (gg Team ottimale)	**IMPORTO** (Esente IVA)
Anno 2023				
L2.S16 – Security Strategy	Analisi della postura di cybersecurity e definizione del piano strategico di potenziamento relativamente ai **servizi IT centralizzati erogati dal Datacenter Principale di ASL Roma 1** (Ambito IT)	L2.S16 — gg/p Team ottimale	**480**	**120.000 €**
L2.S16 – Security Strategy	Cyber Security Awareness: 1) Estensione per 12 mesi dell'attuale progetto di Cyber Security Awareness supportato da relativa piattaforma; 2) Somministrazione di 4 corsi sulla norma ISO 27001	L2.S16 — gg/p Team ottimale	**672**	**168.000 €**
L2.S16 – Security Strategy	Cybersecurity Enforcement relativi alla Cloud Migration NOTA: Progetto attivabile da Luglio 2023	L2.S16 — gg/p Team ottimale	**400**	**100.000 €**
L2.S16 – Security Strategy	Mantenimento NIS e progressiva passaggio/estensione a NIS2	L2.S16 — gg/p Team ottimale	**500**	**125.000 €**
L2.S16 – Security Strategy	Progetto VAPT: Sviluppo evolutivo Portale "Security View"	L2.S16 — gg/p Team ottimale	**280**	**70.000 €**
L2.S22 – Penetration Test	Progetto VAPT: Attività di Vulnerability Assessment & Penetration Testing	L2.S22 – gg/p Team ottimale	**970**	**160.050 €**
Anno 2024				
L2.S16 – Security Strategy	Analisi della postura di cybersecurity e definizione del piano strategico di potenziamento relativamente **ai servizi IT afferenti a max 5 strutture territoriali di media/piccola complessità** (Ambito IT)	L2.S16 — gg/p Team ottimale	**600**	**150.000 €**
L2.S16 – Security Strategy	Cyber Security Awareness: 1) Estensione per 12 mesi dell'attuale progetto di Cyber Security Awareness supportato da relativa piattaforma; 2) Somministrazione di 5 sessioni formative relative a Perimetro Nazionale Sicurezza Cibernetico, NIS, NIS2, IS27001 (Overview) e formazione specialistica cyber	L2.S16 — gg/p Team ottimale	**688**	**172.000 €**
L2.S16 – Security Strategy	Cybersecurity Enforcement relativi alla Cloud Migration	L2.S16 — gg/p Team ottimale	**1120**	**280.000 €**

L2.S16 – Security Strategy	Mantenimento NIS e progressiva passaggio/estensione a NIS2	L2.S16 –– gg/p Team ottimale	**500**	**125.000 €**
L2.S16 – Security Strategy	Progetto VAPT: Sviluppo evolutivo Portale "Security View"	L2.S16 –– gg/p Team ottimale	**280**	**70.000 €**
L2.S22 – Penetration Test	Progetto VAPT: Attività di Vulnerability Assessment & Penetration Testing	L2.S22 – gg/p Team ottimale	**970**	**160.050 €**
Anno 2025				
L2.S16 – Security Strategy	Cybersecurity Enforcement relativi alla Cloud Migration	L2.S16 –– gg/p Team ottimale	**1120**	**280.000 €**
L2.S16 – Security Strategy	Mantenimento NIS e progressiva passaggio/estensione a NIS2	L2.S16 –– gg/p Team ottimale	**500**	**125.000 €**
L2.S22 – Penetration Test	Progetto VAPT: Attività di Vulnerability Assessment & Penetration Testing	L2.S22 – gg/p Team ottimale	**970**	**160.050 €**
			TOTALE (Esclusa IVA)	**2.265.150 €**

4.3 Dettaglio dei servizi richiesti

4.3.1 L2.S16 - Security Strategy

4.3.1.1 Descrizione e caratteristiche del servizio

Anni	Macro-attività	Attività	Deliverable
2023 – 2024 – 2025	**Analisi della postura di cybersecurity e definizione del piano strategico di potenziamento (Ambito IT)**	Esecuzione di una serie di **Assessment di Sicurezza** erogati nei confronti di **diversi contesti e perimetri**, finalizzati all'analisi dei livelli di maturità delle capacità cyber in termini di organizzazione, processi e tecnologie (People, Process & Technology) e successiva identificazione delle principali iniziative che costituiranno i piani strategici dell'Ente in riferimento ai diversi contesti e perimetri, secondo programmi pluriennale e con azioni di rimedio a breve-medio-lungo termine. In termini di perimetri, si sono identificati i seguenti: 1) Servizi IT centralizzati ed erogati dal Datacenter Principali (San Filippo Neri). Nota: verrà considerato un perimetro di analisi che comprenda l'erogazione di un campione di massimo 50 servizi IT che possano considerarsi rappresentativi in termini di complessità e criticità (es: Posta elettronica, File sharing, servizi amministrativi e contabili, ecc); 2) Assessment sui servizi IT afferenti a max 5 strutture territoriali di media/piccola complessità (es: Ospedale Santo Spirito, Ospedale Oftalmico, Santa Maria della Pietà, ecc). Analisi di alto livello sui servizi IT afferenti a max 5 strutture territoriali di media/piccola complessità. Nota: per ogni struttura territoriale verrà considerato un perimetro di analisi che comprenda l'erogazione di un campione di massimo 20 servizi IT che possano considerarsi rappresentativi in termini di complessità e criticità.	• Risultati dell'Assessment (Executive Summary e Detail Report) • Piani Strategici di Sicurezza a breve, medio e lungo termine (Executive Summary e Detail Report)
2023	**Cyber Security Awareness**	1) Progetto di Cyber Security Awareness supportato dalla relativa piattaforma; 2) Somministrazione di 4 corsi sulla norma ISO 27001 (max 10 persone, durata 5 gg) comprensivi di rilascio di attestati di frequenza, esame e certificazione	• Materiale formativo del corso • Attestato di frequenza e certificazione

2024	**Cyber Security Awareness**	1) Progetto di Cyber Security Awareness supportato dalla relativa piattaforma; 3) Somministrazione di 5 sessioni formative (max 10 persone, durata 3 gg) relativi a Perimetro Nazionale Sicurezza Cibernetico, NIS, NIS2, IS27001 (Overview) e formazione specialistica cyber su personale di UOC con rilascio di attestati di frequenza	• Materiale formativo del corso • Attestati di frequenza
2023 (da Settembre) – 2024 – 2025	**Cybersecurity Enforcement relativo alla Cloud Migration**	Servizio di affiancamento alle attività di Cloud Migration (IaaS/PaaS) che ASLR1 sta per intraprendere. Il supporto consiste in analisi puntuale dei requisiti di Cybersecurity di ASLR1 e la definizione dell'organizzazione, dei processi e delle tecnologie di Cloud Security che sarà necessario garantire e predisporre nella migrazione al Cloud per assicurare gli adeguati livelli di Riservatezza, Integrità, Disponibilità e Conformità di dati e servizi migrati nel Cloud. Nel dettaglio i servizi inclusi sono: 1) **Cloud Security Control Library**: Definizione di una libreria di controlli di sicurezza tecnici e organizzativi per gli ambienti cloud che considera i domini application, data, identity, infrastructure, monitoring, response e strategy & governance; 2) **Cloud Security Architecture**: disegno di una Security blueprint architetturale partendo dalle capability di sicurezza attualmente presenti nel contesto onprem, riviste in un'ottica Cloud, e valutando eventuali funzionalità offerte dal CSP al fine di complementare le misure di sicurezza minime necessarie; 3) **Cloud Security Governance framework**: sviluppo di linee guida di security e compliance per l'adozione e l'implementazione sicura dei servizi cloud, e revisione dei principali processi di security in ottica cloud. Il servizio prevede la revisione di 6 processi di gov già esistenti oppure la definizione ex-novo di 3 processi (es: Change Management, Cyber Incident Management, Accesso Control & User Access Management, ecc) 4) **Supporto nella verifica delle configurazioni sicura dell'ambiente Cloud** mediante assessment periodici di Posture Management al fine di governare eventuali misconfiguration lungo la migrazione dei servizi in Cloud NOTA: I servizi elencati sono stati stimati e si riferiscono a: - migrazione dei servizi verso 1 CSP Pubblico (es: AWS, Azure o GCP). Tali valori potrebbero essere rivisti al rialzo nel caso di migrazioni verso CSP diversi da quelli indicati; - un numero massimo di 500 oggetti migrati in Cloud.	• Libreria controlli • 1 Architettura Cloud Sicura • Cloud Security Governance Framework • Cloud Security Posture (2 report mensili) per 12 mesi **NOTA**: nel primo anno (2023) sono previsti esclusivamente i primi due deliverable cioè, Libreria Controlli e 1 Architettura Cloud Sicura). Nel 2024 e 2025 sono invece previsti tutti i deliverable riportati sopra.

2023 – 2024 – 2025	**Mantenimento NIS e progressiva passaggio/estensione a NIS2**	Serie di servizi di indirizzo per la conformità alla NIS e di supporto per il passaggio graduale e all'estensione alla NIS2. I servizi comprendono: 1) Supporto al monitoraggio e reporting (PMO) del remediation plan NIS; 2) Supporto alla revisione/aggiornamento di policy/procedure Cyber per indirizzare i gap; 3) Monitoraggio degli sviluppi normativi in ambito NIS2; 4) Supporto all'analisi delle implicazioni per ASL Roma 1 derivanti dalla NIS2. NOTE: - Si assume che sia già stato effettuato negli anni scorsi un risk/maturity assessment rispetto alle linee guida NIS ministeriali e che sia già disponibile il piano di remediation con gli interventi da implementare. Non è previsto un re-assessment rispetto alle misure, eventualmente indirizzabile con collaborazione specifica; - Non sono previste attività di implementazione di soluzioni/tecnologie, eventualmente indirizzabili con collaborazione specifica; - Le attività di revisione/aggiornamento delle policy/procedure Cyber a di ASL Roma 1 saranno valutate volta per volta, compatibilmente con le attività di PMO in cui il team del fornitore è impegnato. Qualora l'effort richiesto al fornitore non fosse compatibile con le attività di PMO pattuite, le nuove attività potranno essere indirizzate con collaborazione specifica; - Con riferimento alla NIS2, il fornitore fornisce un supporto interpretativo prettamente tecnico, eventuale supporto di natura legale può essere indirizzabile con collaborazione specifica.	• Presentazioni di SAL e reporting executive periodici sullo stato avanzamento del remediation plan • Presentazioni sulla nuova normativa NIS2
2023 – 2024	**Progetto VAPT – Sviluppo evolutivo Portale " Security View "**	Progetto di sviluppo evolutivo ad-hoc sul portale Security View di un servizio di importazione di bollettini di sicurezza provenienti da fonti esterne pubbliche e private con, in particolare, la ricezione periodica delle informative provenienti dalla Polizia dello Stato in un formato testuale concordato e che andranno ad alimentare eventuali azioni di VA e PT. Parallelamente le stesse attività di scansione periodica possono generare notifiche esportabili verso sistemi terzi con lo scopo di alimentare una libreria comune di vulnerabilità in ambito applicativo sanitario. L'attività di import/export di security bullettin sarà possibile direttamente da interfaccia web oltre alla visualizzazione, ricerca e gestione dei dati.	• Import e visualizzazione in dashboard di bollettini di sicurezza • Export, in formato concordato, di un sottoinsieme dei risultati di VA e PT su applicativi sanitari

4.3.1.2 Modalità di erogazione e consuntivazione

Coerentemente a quanto previsto nel "CAPITOLATO TECNICO SPECIALE SERVIZI DI COMPLIANCE E CONTROLLO" si precisa che la modalità di remunerazione di tali servizi è "progettuale (a corpo)" e che la metrica di misurazione è "*giorni/persona del team ottimale*".

Saranno definiti di concerto con l'Amministrazione dei task e dei deliverable, dimensionati e valorizzati economicamente.

La consuntivazione e la relativa fatturazione avverranno con una cadenza mensile alla consegna dei deliverable. Nella tabella sotto la suddivisione dei valori economici relativi ai vari deliverable previsti:

SERVIZIO	MACRO ATTIVITA	DELIVERABLE	VALORE ECONOMICO (Esente IVA)
L2.S16 – Security Strategy	**Anno 2023**		
	Analisi della postura di cybersecurity e definizione del piano strategico di potenziamento (Ambito IT)	A. Risultati dell'Assessment (Executive Summary e Detail Report) B. Piani Strategici di Sicurezza a breve, medio e lungo termine (Executive Summary e Detail Report)	A. **70.000 €** B. **50.000 €**
	Cyber Security Awareness (4 corsi ISO27001)	C. Materiale formativo del corso e Attestato di frequenza e/o certificazione	C. **4 x 7.000 €**
	Cyber Security Awareness (Corsi Cybersecurity supportati da piattaforma)	D. Materiale formativo del corso e Attestato di frequenza e certificazione	D. **140.000 €**
	Cybersecurity Enforcement relativo alla Cloud Migration	E. Libreria controlli F. 1 Architettura Cloud Sicura	E. **60.000 €** F. **40.000 €**
	Mantenimento NIS e progressiva passaggio/estensione a NIS2	G. Presentazioni di SAL e reporting executive periodici sullo stato avanzamento del remediation plan (4/anno) H. Presentazioni sulla nuova normativa NIS2	G. **4 x 25.000 €** H. **25.000 €**
	Progetto VAPT – Sviluppo evolutivo Portale "Security View"	I. Import e visualizzazione in dashboard di bollettini di sicurezza J. Export, in formato concordato, di un sottoinsieme dei risultati di VA e PT su applicativi sanitari	I. **40.000 €** J. **30.000 €**

SERVIZIO	MACRO ATTIVITA	DELIVERABLE	VALORE ECONOMICO (Esente IVA)
	Anno 2024		
	Analisi della postura di cybersecurity e definizione del piano strategico di potenziamento (Ambito IT)	K. Risultati dell'Assessment (Executive Summary e Detail Report) L. Piani Strategici di Sicurezza a breve, medio e lungo termine (Executive Summary e Detail Report)	K. **90.000 €** L. **60.000 €**
	Cyber Security Awareness (5 corsi Perimetro Sicurezza Nazionale, NIS, /NIS2)	M. Materiale formativo del corso e Attestati di frequenza	M. **5 x 6.400 €**
	Cyber Security Awareness (Corsi Cybersecurity supportati da piattaforma)	N. Materiale formativo del corso e Attestato di frequenza e/o certificazione	N. **140.000 €**
	Cybersecurity Enforcement relativo alla Cloud Migration	O. Libreria controlli P. 1 Architettura Cloud Sicura Q. Cloud Security Governance Framework R. Cloud Security Posture (2 report mensili) per 12 mesi	O. **60.000 €** P. **40.000 €** Q. **110.000 €** R. **70.000**
	Mantenimento NIS e progressiva passaggio/estensione a NIS2	S. Presentazioni di SAL e reporting executive periodici sullo stato avanzamento del remediation plan (4/anno) T. Presentazioni sulla nuova normativa NIS2	S. **4 x 25.000 €** T. **25.000 €**
	Progetto VAPT – Sviluppo evolutivo Portale "Security View "	U. Import e visualizzazione in dashboard di bollettini di sicurezza V. Export, in formato concordato, di un sottoinsieme dei risultati di VA e PT su applicativi sanitari	U. **40.000 €** V. **30.000 €**
	Anno 2025		
	Cybersecurity Enforcement relativo alla Cloud Migration	W. Libreria controlli X. 1 Architettura Cloud Sicura Y. Cloud Security Governance Framework Z. Cloud Security Posture (2 report mensili) per 12 mesi	W. **60.000 €** X. **40.000 €** Y. **110.000 €** Z. **70.000**
	Mantenimento NIS e progressiva passaggio/estensione a NIS2	AA. Presentazioni di SAL e reporting executive periodici	AA. **4 x 25.000 €** BB. **25.000 €**

SERVIZIO	MACRO ATTIVITA	DELIVERABLE	VALORE ECONOMICO (Esente IVA)
		sullo stato avanzamento del remediation plan (4/anno) BB. Presentazioni sulla nuova normativa NIS2	
TOTALE			**1.785.000 €**

Il team di lavoro per la realizzazione delle attività sopraccitate prevede il coinvolgimento delle seguenti figure professionali:

- Security Principal
- Security Solution Architect
- Senior Information Security Consultant
- Senior Security Auditor
- Data Protection Specialist

Le attività potranno essere erogate presso varie sedi di Roma dell'Amministrazione Contraente o da remoto presso le sedi del RTI.

4.3.1.3 Attivazione e durata

Si prevede l'avvio del servizio entro il Q1 2023 per una durata di 36 mesi.

4.3.2 L2.S22 – Penetration Test

4.3.2.1 Descrizione e caratteristiche del servizio

Anni	Macro-attività	Attività	Deliverable
2023 – 2024 – 2025	**Progetto VAPT – Vulnerability Assessment e Penetration Testing**	Progetto di Vulnerability Assessment (VA) che prevede la procedura di enumerazione servizi esposti per ogni IP e per ogni FQDN oggetto di Assessment, e ricerca delle vulnerabilità note per ogni servizio rilevato. Il progetto prevede: 1) un piano di "Scanning" mensile da Internet su sistemi esterni (Data Center e Cloud); 2) un piano di "Scanning" semestrale da rete locale su sistemi interni (fino a 20 IP a campione). 3) esecuzione in modalità "on-demand" di simulazioni dei tentativi di accesso ai sistemi/servizi/applicazioni "Penetration Test" (PT), sfruttando le vulnerabilità rilevate nella fase precedente di VA, sui servizi che si decide di approfondire. I risultati delle attività di VA e PT potranno essere esposti attraverso il portale di sicurezza denominato "Security View". Nel progetto vengo incluse anche alcune attività relative alla soluzione già in uso presso ASL, di Mail Security di frontiera LibraEsva. Tali attività permetteranno la raccolta e l'indicizzazione dei log collezionati dalla piattaforma che verranno poi organizzate in opportuni report utili ad evidenziare vulnerabilità ed anomalie potenzialmente critiche (es: tentativi non autorizzati di accesso, traffico anomalo, attacchi virali o violazione delle policy) e identificare gli IOC (Indicator Of Compromise) e per estensione anche gli IOA (Indicator Of Attack).	• Vulnerability Report: vulnerabilità per ogni singolo host con relativo trend basato sulla storicizzazione degli scan effettuati. • Remediation Plan: viene presentato il piano di azioni da percorrere per la messa in sicurezza delle vulnerabilità rilevate. • Mail Security Report utili ad evidenziare vulnerabilità ed anomalie potenzialmente critiche e IOC/IOA

4.3.2.2 Modalità di erogazione e consuntivazione

Coerentemente a quanto previsto nel "CAPITOLATO TECNICO SPECIALE SERVIZI DI COMPLIANCE E CONTROLLO" si precisa che la modalità di remunerazione di tali servizi è "progettuale (a corpo)" e che la metrica di misurazione è "*giorni/persona*".

Saranno definiti di concerto con l'Amministrazione dei task e dei deliverable, dimensionati e valorizzati economicamente.

La consuntivazione e la relativa fatturazione avverranno con una cadenza mensile alla consegna dei deliverable. Nella tabella sotto la suddivisione dei valori economici relativi ai vari deliverable previsti:

SERVIZIO	MACRO ATTIVITA	DELIVERABLE	VALORE ECONOMICO (Esente IVA)
L2.S22 – Penetration Test	**Anno 2023**		
	Progetto VAPT – Vulnerability Assessment e Penetration Testing	CC. Vulnerability Report: vulnerabilità per ogni singolo host con relativo trend basato sulla storicizzazione degli scan effettuati. Remediation Plan: viene presentato il piano di azioni da percorrere per la messa in sicurezza delle vulnerabilità rilevate. Mail Security Report utili ad evidenziare vulnerabilità ed anomalie potenzialmente critiche e IOC/IOA	CC. **160.050 €**
	Anno 2024		
	Progetto VAPT – Vulnerability Assessment e Penetration Testing	DD. Vulnerability Report: vulnerabilità per ogni singolo host con relativo trend basato sulla storicizzazione degli scan effettuati. Remediation Plan: viene presentato il piano di azioni da percorrere per la messa in sicurezza delle vulnerabilità rilevate. Mail Security Report utili ad evidenziare vulnerabilità ed anomalie potenzialmente critiche e IOC/IOA	DD. **160.050 €**
	Anno 2025		
	Progetto VAPT – Vulnerability Assessment e Penetration Testing	EE. Vulnerability Report: vulnerabilità per ogni singolo host con relativo trend basato sulla storicizzazione degli scan effettuati. Remediation Plan: viene presentato il piano di azioni da percorrere per la messa in	EE. **160.050 €**

SERVIZIO	MACRO ATTIVITA	DELIVERABLE	VALORE ECONOMICO (Esente IVA)
		sicurezza delle vulnerabilità rilevate. Mail Security Report utili ad evidenziare vulnerabilità ed anomalie potenzialmente critiche e IOC/IOA	
TOTALE			**480.150 €**

Il team di lavoro per la realizzazione delle attività sopraccitate prevede il coinvolgimento delle seguenti figure professionali:

- Security Principal
- Senior Penetration tester
- Junior Penetration tester
- Forensic Expert

Le attività potranno essere erogate presso varie sedi di Roma dell'Amministrazione Contraente o da remoto presso le sedi del RTI.

4.3.2.3 Attivazione e durata

Si prevede l'avvio del servizio entro Q1 2023 per una durata di 36 mesi.

5 Organizzazione e modalità di erogazione del contratto esecutivo

5.1 Organizzazione e figure di riferimento dell'amministrazione

I principali punti di contatto tecnici dell'amministrazione per l'esecuzione del presente progetto sono il Direttore UOC Sistemi e tecnologie informatiche e di comunicazione, il Responsabile della transizione digitale, il Referente NIS e il Referente tecnico NIS.

L'amministrazione si riserva di poter identificare durante l'esecuzione del contratto ulteriori figure di riferimento con le quali il fornitore potrà interfacciarsi.

5.2 Attività in carico alle aziende del RTI

Nell'ambito della specifica fornitura le attività saranno svolte dalle aziende secondo la ripartizione seguente:

SERVIZIO	Deloitte Risk Advisory	EY Advisory	Teleco
L2.S16	44,1 %	34,7 %	0 %
L2.S22	0 %	21,2 %	0 %
TOTALE	**44,1 %**	**55,9 %**	**0 %**

5.3 Organizzazione e figure di riferimento del fornitore

In relazione all'organizzazione e alle figure di riferimento del Fornitore per la conduzione del progetto, si prevede la presenza di un RUAC con una struttura di Governance a supporto per le attività di PMO. In particolare, il **RUAC del CE** collabora con il RUAC di AQ ed è responsabile dei servizi del singolo CE.

Per l'erogazione dei servizi è prevista la presenza del referente tecnico per ciascun CE e comunque per ciascuna Amministrazione per tutti i servizi del Lotto 2 - Referente Tecnico CE (RT) - che assicura il corretto svolgimento dei servizi ed il relativo livello di qualità di erogazione, nel pieno rispetto degli indicatori condivisi. Per ciascun servizio oggetto del presente Piano Operativo, l'organizzazione prevede la composizione di un gruppo dedicato composto da un **Responsabile Attività** e da un gruppo di lavoro di supporto.

RUOLO	NOMINATIVI
RUAC CE	Fabio Battelli (Deloitte)
Referente Tecnico CE	Marco Ceccon (Deloitte)
Responsabile Attività L2.S16	Marco Ceccon (Deloitte)
Responsabile Attività L2.S22	Samuele Moretti (EY)

5.4 Modalità di esecuzione dei servizi

Le attività relative all'esecuzione dei servizi saranno svolte presso gli uffici del Fornitore e, ove necessario e/o richiesto per l'espletamento delle attività contrattuali, presso l'Amministrazione, nel rispetto della normativa sanitaria.

6 PIANO DI LAVORO

6.1 Piano di Presa in carico

Il piano di presa in carico si basa sul 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.

FASE	ATTIVITÀ L2.S16
1. Analisi della postura di cybersecurity e definizione del piano strategico di potenziamento (Ambito IT)	• Risultati dell'Assessment (Executive Summary e Detail Report) • Piani Strategici di Sicurezza a breve, medio e lungo termine (Executive Summary e Detail Report)
2. Cyber Security Awareness	• Materiale formativo del corso • Attestato di frequenza e certificazione
3. Cyber Security Awareness	• Materiale formativo del corso • Attestati di frequenza
4. Cybersecurity Enforcement relativo alla Cloud Migration	• Libreria controlli • 1 Architettura Cloud Sicura • Cloud Security Governance Framework • Cloud Security Posture (2 report mensili) per 12 mesi
5. Mantenimento NIS e progressiva passaggio/estensione a NIS2	• Presentazioni di SAL e reporting executive periodici sullo stato avanzamento del remediation plan • Presentazioni sulla nuova normativa NIS2
6. Progetto VAPT – Sviluppo evolutivo Portale "Security View "	• Import e visualizzazione in dashboard di bollettini di sicurezza • Export, in formato concordato, di un sottoinsieme dei risultati di VA e PT su applicativi sanitari

FASE	ATTIVITÀ L2.S22
1. Progetto VAPT – Vulnerability Assessment e Penetration Testing	• Vulnerability Report: vulnerabilità per ogni singolo host con relativo trend basato sulla storicizzazione degli scan effettuati • Remediation Plan: viene presentato il piano di azioni da percorrere per la messa in sicurezza delle vulnerabilità rilevate • Mail Security Report utili ad evidenziare vulnerabilità ed anomalie potenzialmente critiche e IOC/IOA

6.2 Cronoprogramma

La durata ipotizzata per la fornitura è di 36 mesi dalla data di attivazione, compatibilmente con il vincolo definito dall'Accordo Quadro, ovvero che i Contratti Esecutivi hanno una durata massima pari alla durata residua, al momento della sua stipula, dell'Accordo Quadro.

Di seguito si riporta la pianificazione di massima del programma con indicazione degli obiettivi in ambito del presente piano.

Obiettivi/Servizi	Anno 2023				Anno 2024				Anno 2025			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
L2.S16												
L2.S22												

6.3 Data di attivazione e durata del servizio

Si prevede l'avvio del servizio entro Q1 2023 per una durata di circa 36 mesi.

7 Piano della qualità specifico

7.1 Organizzazione dei Servizi

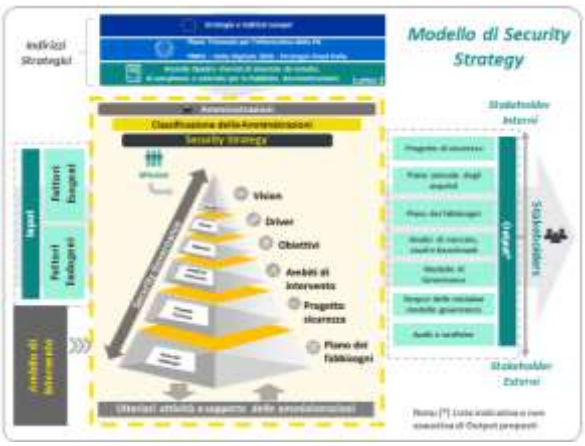
A Livello di gestione del contratto esecutivo sono state identificate le seguenti figure con le relative responsabilità:

- 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, assicura 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 è referente tecnico per ciascuna attività all'interno del CE, coordina e assicura il corretto svolgimento delle attività operative eseguite dal team di lavoro.
- Team di Lavoro (TL), team operativi di intervento impegnati nell'erogazione dei servizi, composti da professionisti con profili previsti.

7.2 Metodologie e Tecniche

Security Strategy (L2.S16)

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.
L'approccio concreto di elaborazione del Progetto di Sicurezza (di seguito PdS) avviene tramite modelli di PdS differenziati sulla base della classificazione e della complessità delle Amministrazioni (MappaPA).
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.

Penetration Test (L2.S22)

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**.

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.