SISTEMA SANITARIO REGIONALE
ASL ROMA 1

DELIBERAZIONE DEL DIRETTORE GENERALE

N. 410 **del** 14/04/2025

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 Consulting S.r.l. S.B. (Mandataria), per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni per le esigenze della Asl Roma 1, per un periodo di 48 mesi - Importo complessivo pari ad € 1.600.000,00 iva esclusa pari ad € 1.952.000,00 iva inclusa + € 14.400,00 per accantonamento incentivi funzioni tecniche, ex art. 113 del D. Lgs. n. 50/2016 Codice dei Contratti Pubblici.

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

Centro di Costo: BD07 L'Estensore:Dott.ssa 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
Dott. GIUSEPPE GUARNIERI	Dott. MASSIMILIANO COLTELLACCI	Ing. PAOLA BRAZZODURO
Firmatario: GIUSEPPE GUARNIERI Data: 09/04/2025 17:40:26 CEST	Firmatario: MASSIMILIANO COLTELLACCI Data: 09/04/2025 17:44:34 CEST	Firmatario: PAOLA BRAZZODURO Data: 10/04/2025 09:25:43 CEST

Il funzionario addetto al controllo di budget, con la sottoscrizione del presente atto, attesta che lo stesso 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
€366.000,00	2025	CE	502020106	Servizi di Assistenza informatica	Dott. Massimiliano Coltellacci	Si
€14.400,00	2025	CE	516040605	accantonamenti incentivi funzioni tecniche art.113 D.Lgs. n. 50/2016	Dott. Massimiliano Coltellacci	No
€488.000,00	2026	CE	502020106	Servizi di Assistenza informatica	Dott. Massimiliano Coltellacci	No
€488.000,00	2027	CE	502020106	Servizi di Assistenza informatica	Dott. Massimiliano Coltellacci	No
€488.000,00	2028	CE	502020106	Servizi di Assistenza informatica	Dott. Massimiliano Coltellacci	No
€122.000,00	2029	CE	502020106	Servizi di Assistenza informatica	Dott. Massimiliano Coltellacci	No

Il Funzionario addetto al controllo di budget

Dott. MASSIMILIANO COLTELLACCI

Firmatario: MASSIMILIANO COLTELLACCI
Data: 09/04/2025 17:44:58 CEST

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 nota prot. n. 34857 del 26/02/2025

Firmatario: GIORGIO BACCARI
Data: 11/04/2025 15:09:05 CEST

Parere del Direttore Amministrativo Dr. Francesco Quagliariello

Favorevole

Firmatario: FRANCESCO QUAGLIARIELLO
Data: 14/04/2025 13:46:31 CEST

(con motivazioni allegate al presente atto)
Non favorevole

Parere del Direttore Sanitario Dr. Gennaro D'Agostino

Favorevole

Firmatario: GENNARO D'AGOSTINO
Data: 14/04/2025 13:54:04 CEST

(con motivazioni allegate al presente atto)
Non favorevole

Il presente provvedimento si compone di n.46 pagine di cui n. 0 pagine di allegati

Il Direttore Generale
Dr. Giuseppe Quintavalle

Firmatario: GIUSEPPE QUINTAVALLE
Data: 14/04/2025 14:27:27 CEST

REGIONE LAZIO

SISTEMA SANITARIO REGIONALE
ASL ROMA 1

IL DIRETTORE SOSTITUTO 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;

VISTO il Decreto del Presidente della Regione Lazio T00006 del 10 gennaio 2025 con il quale è stato nominato Direttore Generale dell'Azienda Sanitaria Locale Roma 1, il dott. Giuseppe Quintavalle;

l'atto di autonomia Aziendale approvato con Deliberazione n. 1153 del 17 dicembre 2019, approvato con Decreto del Commissario ad Acta n. U00020 del 27 gennaio 2020 e pubblicato sul BURL del 30 gennaio 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 Deliberazione n. 138 del 25/02/2025 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. 36 del 31 marzo 2023 "Codice dei contratti pubblici" nel quale è previsto, all'art. 226 comma 2, che a decorrere dalla data in cui il codice acquista efficacia ai sensi dell'articolo 229, comma 2, le disposizioni di cui al decreto legislativo n. 50 del 2016 continuano ad applicarsi ai procedimenti in corso e che per procedimenti in corso, rientrano, tra gli altri, le procedure e i contratti per i quali i bandi o avvisi con cui si indice la procedura di scelta del contraente siano stati pubblicati prima della data in cui il codice acquista efficacia;

PREMESSO CHE con Delibera n. 262 del 03/03/2023 la Asl Roma 1 aderiva 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), in scadenza al 03/03/2026;

CONSIDERATO che l'Asl si pone l'obiettivo di aumentare la conoscenza e la consapevolezza sui rischi cyber inerenti alla propria organizzazione e ai propri servizi e infrastrutture informatiche poiché le stesse rivestono un'importanza centrale, così come programmare le azioni da attuare per mitigare i rischi cyber e per contrastare eventi di cybercrime;

che allo scopo di innovare i servizi ed incrementare la produttività dell'Amministrazione, la

Sicurezza dei sistemi e 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;

ALTRESI'

che emergono nuove esigenze di sicurezza delle Informazioni e delle Infrastrutture dovute al mutamento degli scenari di rischio, delle nuove minacce e dell'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);

che si rende necessario adottare una visione strategica di lungo periodo e definire 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 2, Direttive ENISA, ecc.);

che lo scenario normativo in cui il l'ASL opera, prevede la Normativa Europea, la Direttiva NIS 2, recepita dall'Italia con il D.Lgs 138/24, il Cyber Security Act, il DL 105/2019 "Perimetro di sicurezza cibernetica" e la L.90/24 (c.d. "Legge Cyber") che sottolineano l'importanza dell'attenzione al fenomeno delcybercrime, il quale è in costante aumento anche nell'ambito PA;

che in tale contesto l'Ente si propone di attuare i seguenti interventi, finalizzati al conseguimento di alcuni importanti obiettivi:

- Attuazione di un processo di "Cybersecurity Re-Enforcement" relativa alle attività di Cloud Migration di alcuni servizi IT erogati dall'ASL Roma 1;
- Definizione e consolidamento KPI di Cybersicurezza negli ambienti Multi/Hybrid-Cloud e dell'efficienza operativa legata ai Medical Device;
- Mantenimento del sistema di conformità a Leggi e Regolamenti (es: D.Lgs 138/2024, Legge 90/24, GDPR, ecc.

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 centraliregionali 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 pertanto l'azienda intende avvalersi della suddetta Convenzione per reperire i servizi aggiuntivi suindicati;

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 Consulting S.r.l. S.B. 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 2025				
L2.S16 – Security Strategy	S16 – 1 Supporto nell'evoluzione e nell'integrazione dei processi operativi relativi al monitoraggio dei livelli di sicurezza e dei livelli di efficienza operativa dei medical device negli ambienti Multi/Hybri-Cloud e IoMT di ASL Roma 1	L2.S16 — gg/p Team ottimale	1200	300.000 €
L2.S16 – Security Strategy	S16 – 2 Supporto su tematiche di Conformità Normativa (*Legge 90/2024*) e su esigenze amministrative verso ACN	L2.S16 — gg/p Team ottimale	400	100.000 €
Anno 2026				

L2.S16 – Security Strategy	S16 – 3 Supporto all'indirizzo strategico, programmatico, tecnico, organizzativo, procedurale ed operativo della Cybersecurity e della Conformità Normativa (*NIS2/D.Lgs 138/24 - Legge 90/2024*)	L2.S16 — gg/p Team ottimale	1600	400.000 €
Anno 2027				
L2.S16 – Security Strategy	S16 – 3 Supporto all'indirizzo strategico, programmatico, tecnico, organizzativo, procedurale ed operativo della Cybersecurity e della Conformità Normativa (*NIS2/D.Lgs 138/24 - Legge 90/2024*)	L2.S16 — gg/p Team ottimale	1600	400.000 €
Anno 2028				
L2.S16 – Security Strategy	S16 – 3 Supporto all'indirizzo strategico, programmatico, tecnico, organizzativo, procedurale ed operativo della Cybersecurity e della Conformità Normativa (*NIS2/D.Lgs 138/24 - Legge 90/2024*)	L2.S16 — gg/p Team ottimale	1600	400.000 €
			TOTALE (Esclusa IVA)	1.600.000 €

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 48 mesi e per un importo complessivo di € 1.600.000,00 IVA esclusa, in conformità al piano operativo allegato;

che la richiesta di CIG per procedure assoggettate al decreto legislativo n. 36/2023, pubblicate a partire dal 01/01/2024, avviene attraverso le piattaforme di approvvigionamento digitale certificate mediante interoperabilità con i servizi erogati dalla PCP attraverso la Piattaforma Digitale Nazionale Dati (PDND);

RICHIAMATA la delibera ANAC n. 582 del 13 dicembre 2023 avente ad oggetto Adozione comunicato relativo all'avvio del processo di digitalizzazione nella quale è previsto l'utilizzo dell'interfaccia web della Piattaforma contratti pubblici per l'acquisizione di CIG per adesione ad accordi quadro e convenzioni i cui bandi siano stati pubblicati entro il 31/12/2023 con o senza successivo confronto competitivo;

DATO ATTO quindi che il Codice Identificativo di Gara (CIG) verrà acquisito mediante la PCP, successivamente al perfezionamento del presente atto;

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 € 14.400,00 (di cui € 2.880,00 quota Fondo innovazione) così distribuito:

Programmazione spesa per investimenti		**5%**	**Se dirigente economia ad eccezione PNRR 2023-2026 come previsto dall'art.8 dlg 13/2023**
a) RUP	-	70%	economia
b) Collaboratore/i RUP	288,00	30%	
	288,00		
Valutazione preventiva dei progetti		**15%**	
a) RUP	-	70%	economia
b) Collaboratore/i RUP	864,00	30%	
	864,00		
Predisposizione e controllo procedure di gare		**20%**	
a) RUP	-	70%	economia
b) Collaboratore/i RUP	960,00	25%	
c) Definizione capitolato	192,00	5%	
	1.152,00		
Esecuzione dei contratti pubblici		**60%**	
a) RUP	-	20%	economia
b) Collaboratore/i RUP	1.152,00	10%	
c) Direttore dell'esecuzione	4.608,00	40%	
d) Collaboratore /i DEC	1.728,00	15%	
e) Incaricato della verifica o certificazione regolare esecuzione	1.382,40	12%	
f) Collaboratore /i dell'incaricato punto e)	345,60	3%	
	9.216,00		
	11.520,00		
quota per incentivazione funzioni	11.520,00	80%	
Fondo innovazione	2.880,00	20%	
	14.400,00	**100%**	

RITENUTO di contabilizzare, al netto degli incentivi, l'importo derivante dal presente provvedimento di € 1.600.000,00 iva esclusa pari ad € 1.952.000,00 iva inclusa sul CE. n. 502020106 "Servizi di Assistenza informatica" - cosi suddiviso:

€ 366.000,00 iva inclusa - Bilancio 2025;
€ 488.000,00 iva inclusa - Bilancio 2026;
€ 488.000,00 iva inclusa - Bilancio 2027;
€ 488.000,00 iva inclusa - Bilancio 2028;
€ 122.000,00 iva inclusa - Bilancio 2029;

che, pertanto, il CE 502020106 per l'anno 2025 presenta la seguente situazione economica:

Budget assegnato	€ 18.500.000,00
Budget già impegnato	€ 18.636.632,35
Importo impegnato con il presente atto	€ 366.000,00

Scostamento - € 502.632,35

che con riferimento allo scostamento negativo, si precisa che lo stesso deriva dalla contabilizzazione di contratti avviati, la cui spesa, a fronte del budget definitivo assegnato ai CCS con nota prot. n. 34857 del 26/02/2025, non può essere ridotta;

di indicare come Responsabile del Procedimento il Dott. Giuseppe Guarnieri, Dirigente della UOC Sistemi e Tecnologie Informatiche e di Comunicazione; di indicare come DEC il Sig. Stefano Scaramuzzino, nei confronti dei quali non sussistono situazioni di conflitto di interesse ex art. 36 D.lgs n. 36/2023;

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 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 Consulting S.r.l. S.B. (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 € 1.600.000,00 iva esclusa pari ad € 1.952.000,00 iva inclusa per un periodo di 48 mesi;

di contabilizzare l'importo derivante dal presente provvedimento, al netto degli incentivi alle funzioni tecniche, pari ad € 1.600.000,00 iva esclusa pari ad € 1.952.000,00 iva inclusa sul CE. n. 502020106 "Servizi di Assistenza informatica" - cosi suddiviso:

€ 366.000,00 iva inclusa - Bilancio 2025;
€ 488.000,00 iva inclusa - Bilancio 2026;
€ 488.000,00 iva inclusa - Bilancio 2027;
€ 488.000,00 iva inclusa - Bilancio 2028;
€ 122.000,00 iva inclusa - Bilancio 2029;

di contabilizzare altresì l'importo di € 14.400,00 quale quota incentivi art.45, commi 3, sul CE "516040605 accantonamenti incentivi funzioni tecniche art.113 D.Lgs. n. 50/2016" sul Bilancio 2025 da liquidarsi successivamente con apposito provvedimento;

di indicare come Responsabile del Procedimento il Dott. Giuseppe Guarnieri, Dirigente della UOC Sistemi e Tecnologie Informatiche e di Comunicazione; di indicare come DEC il Sig. Stefano Scaramuzzino, nei confronti dei quali non sussistono situazioni di conflitto di interesse ex art. 36 D.lgs n. 36/2023;

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 Sostituto della U.O.C. Sistemi e Tecnologie Informatiche e di Comunicazione	Il Direttore Dipartimento Tecnico Patrimoniale
Dott. Giuseppe Guarnieri	Dott. Massimiliano Coltellacci	Ing. Paola Brazzoduro

IL DIRETTORE GENERALE

IN VIRTÚ dei poteri previsti:

- dall'art. 3 del D. Lgs. n. 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 conferitigli con Decreto del Presidente della Regione Lazio n. T00006 del 10 gennaio 2025;

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 Consulting S.r.l. S.B. (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, per un periodo di 48 mesi - Importo complessivo pari ad € 1.600.000,00 iva esclusa pari ad € 1.952.000,00 iva inclusa + € 14.400,00 per accantonamento incentivi funzioni tecniche, ex art. 113 del D. Lgs. n. 50/2016 Codice dei Contratti Pubblici." 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 Consulting S.r.l. S.B. (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 € 1.600.000,00 iva esclusa pari ad € 1.952.000,00 iva inclusa per un periodo di 48 mesi;

di contabilizzare l'importo derivante dal presente provvedimento, al netto degli incentivi alle funzioni tecniche, pari ad € 1.600.000,00 iva esclusa pari ad € 1.952.000,00 iva inclusa sul CE. n. 502020106 "Servizi di Assistenza informatica" - cosi suddiviso:

€ 366.000,00 iva inclusa - Bilancio 2025;

€ 488.000,00 iva inclusa - Bilancio 2026;
€ 488.000,00 iva inclusa - Bilancio 2027;
€ 488.000,00 iva inclusa - Bilancio 2028;
€ 122.000,00 iva inclusa - Bilancio 2029;

di contabilizzare altresì l'importo di € 14.400,00 quale quota incentivi art.45, commi 3, sul CE "516040605 accantonamenti incentivi funzioni tecniche art.113 D.Lgs. n. 50/2016" sul Bilancio 2025 da liquidarsi successivamente con apposito provvedimento;

di indicare come Responsabile del Procedimento il Dott. Giuseppe Guarnieri, Dirigente della UOC Sistemi e Tecnologie Informatiche e di Comunicazione; di indicare come DEC il Sig. Stefano Scaramuzzino, nei confronti dei quali non sussistono situazioni di conflitto di interesse ex art. 36 D.lgs n. 36/2023;

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
Dott. Giuseppe Quintavalle
Firmata digitalmente

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

Data: 13/03/2025

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 Re-Enforcement

Costituito

Raggruppamento Temporaneo di Imprese

composto da:

Deloitte Consulting S.r.l. S.B.

EY Advisory S.p.A.

Teleco S.r.l.

Deloitte. EY teleco

SOMMARIO

1 Introduzione 3
1.1 Ambito 3
1.2 Richieste dell'Amministrazione contraente 3
1.3 Riferimenti 4
1.4 Acronimi e glossario 4
2 Anagrafica dell'amministrazione 5
3 Contesto di riferimento 6
3.1 Contesto dei servizi 6
3.2 Contesto tecnico ed operativo 6
3.3 Contesto Economico – Finanziario 7
3.4 Ambiti funzionali oggetto di intervento 7
3.5 Obiettivi e benefici da perseguire 7
3.6 Categorizzazione dell'intervento 8
3.6.1 Categorizzazione di I livello 8
3.6.2 Categorizzazione di II livello 9
4 Servizi richiesti 11
4.1 Dettaglio dei servizi richiesti 12
4.1.1 L2.S16 – Security Strategy 12
4.2 Organizzazione e figure di riferimento dell'amministrazione 16
4.3 Organizzazione e figure di riferimento del fornitore 16
5 Elementi quantitativi e qualitativi per il dimensionamento servizi 17
5.1 Elementi quantitativi dei servizi 17
5.2 Elementi qualitativi dei servizi 17
5.3 Pianificazione dei servizi 17

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 Consulting S.r.l. S.B. 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 35 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****;*

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 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, Legge 90/2024 Direttiva NIS2 / D.Lgs 138/2024, Direttive ENISA, ecc.).

Lo scenario normativo in cui il l'ASL opera prevede la Normativa Europea, la Direttiva NIS2/D.Lgs. 138_24, la Legge 90_24 (Legge Cyber), 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) 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 e conformità 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 siano 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.

3.4 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:

- Attuazione di un processo di "Cybersecurity Re-Enforcement" relativa alle attività di Cloud Migration di alcuni servizi IT erogati dall'ASL Roma 1;
- Definizione e consolidamento KPI di Cybersicurezza negli ambienti Multi/Hybrid-Cloud e dell'efficienza operativa legata ai Medical Device;
- Mantenimento del sistema di conformità a Leggi e Regolamenti (es: D.Lgs 138/2024, Legge 90/24, GDPR, ecc;

3.5 Obiettivi e benefici da perseguire

Il Progetto di Sicurezza illustrato in questo documento mira ad un costante e crescente livello di maturità del sistema di gestione della sicurezza dell'Ente. La definizione di requisiti e controlli di sicurezza per il

monitoraggio dell'ambiente ibrido dell'Ente potranno elevare il livello di efficacia dei presidi di cybersicurezza, al fine di fronteggiare in maniera più efficace i rischi cyber.

3.6 Categorizzazione dell'intervento

3.6.1 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

3.6.2 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

4 Servizi richiesti

SERVIZI RICHIESTI				
ID	**NOME SERVIZIO**	**VOCE DI COSTO**	**QUANTITA'** (gg Team ottimale)	**IMPORTO** (Esente IVA)
Anno 2025				
L2.S16 – Security Strategy	**S16 – 1** Supporto nell'evoluzione e nell'integrazione dei processi operativi relativi al monitoraggio dei livelli di sicurezza e dei livelli di efficienza operativa dei medical device negli ambienti Multi/Hybri-Cloud e IoMT di ASL Roma 1	L2.S16 — gg/p Team ottimale	**1200**	**300.000 €**
L2.S16 – Security Strategy	**S16 – 2** Supporto su tematiche di Conformità Normativa (*Legge 90/2024*) e su esigenze amministrative verso ACN	L2.S16 — gg/p Team ottimale	**400**	**100.000 €**
Anno 2026				
L2.S16 – Security Strategy	**S16 – 3** Supporto all'indirizzo strategico, programmatico, tecnico, organizzativo, procedurale ed operativo della Cybersecurity e della Conformità Normativa (*NIS2/D.Lgs 138/24 - Legge 90/2024*)	L2.S16 — gg/p Team ottimale	**1600**	**400.000 €**
Anno 2027				
L2.S16 – Security Strategy	**S16 – 3** Supporto all'indirizzo strategico, programmatico, tecnico, organizzativo, procedurale ed operativo della Cybersecurity e della Conformità Normativa (*NIS2/D.Lgs 138/24 - Legge 90/2024*)	L2.S16 — gg/p Team ottimale	**1600**	**400.000 €**
Anno 2028				
L2.S16 – Security Strategy	**S16 – 3** Supporto all'indirizzo strategico, programmatico, tecnico, organizzativo, procedurale ed operativo della Cybersecurity e della Conformità Normativa (*NIS2/D.Lgs 138/24 - Legge 90/2024*)	L2.S16 — gg/p Team ottimale	**1600**	**400.000 €**
			TOTALE (Esclusa IVA)	**1.600.000 €**

4.1 Dettaglio dei servizi richiesti

4.1.1 L2.S16 – Security Strategy

4.1.1.1 Descrizione e caratteristiche del servizio

Anni	Attività	Dettagli sulle attività	Deliverable
2025	S16-1 – Supporto nell'evoluzione e nell'integrazione dei processi operativi relativi al monitoraggio dei livelli di sicurezza e dei livelli di efficienza operativa dei medical device negli ambienti Multi/Hybri-Cloud e IoMT di ASL Roma 1	Le attività in questione hanno il fine di supportare il miglioramento continuo dei macro-processi di controllo e verifica della cybersicurezza e dell'efficienza operativa degli elettromedicali in ambienti Multi/Hybri-Cloud e IoMT di ASL Roma 1. Il servizio si esplicita nella serie di attività elencate qui di seguito: • Identificazione di tutte le fonti che possono concorrere ad alimentare il Data Lake di ASL Roma 1 e che possono essere utili all'evoluzione delle dashboard di cybersecurity e di efficienza operativa; • Ingegnerizzazione del sistema di raccolta ed elaborazione dei dati nel Data Lake anche in funzione di possibili integrazioni con altri sistemi di Business Intelligence già in fase di sviluppo presso ASL Roma 1. Nota: allo stato attuale il Data Lake raccoglie dati dalle seguenti fonti: ○ Claroty xDome (ex Medigate) ○ Security View (Asset Inventory + risultanze VAPT) ○ Web Application Firewall (WAF) ○ Moduli Fortinet (Firewall, Multi Factor Autentication, Priviledge Account Management, Network Access Control) • Definizione e sviluppo della metodologia di correlazione degli eventi, funzionale allo sviluppo di KPI/reporting di supporto alle decisioni • Armonizzazione col sistema di VAPT ampliato ai medical device sul perimetro cyber • Supporto alla definizione delle specifiche tecniche utili alla visualizzazione dei KPI di Cybersecurity e di efficienza operativa dei dispositivi elettromedicali (per successive implementazioni su sistemi di dashboarding/reporting esistenti o eventuali sistemi di Business Intelligence in uso/futuri) • Integrazione di Dashboard utili a rappresentare l'andamento di un max di ulteriori 20 KPI rispetto alle attuali.	• Elenco nuove fonti • Descrizione del data Lake di raccolta dati • Metodologia correlazione eventi • Formalizzazione e/o aggiornamento nuovi KPI di sicurezza e di efficienza operativa (c.ca 50) • Specifiche tecniche per visualizzazione KPI su sistemi di dashboarding e/o di Business Intelligence • Dashboard per ulteriori 20 KPI.

2025	**S16-2 – Supporto su tematiche di Conformità Normativa (Legge 90/2024) e su esigenze amministrative verso ACN**	Servizio continuativo strategico e gestionale comprensivo delle seguenti attività: • Monitoraggio e reporting (PMO) nelle attività legate alla conformità Legge 90/2024 • Analisi delle implicazioni per ASL Roma 1 derivanti dalla Legge 90/2024 e sue evoluzioni • Supporto e consulenza relativamente alla eventuale attivazione di presidi tecnologici ed organizzativo-procedurali utili ad indirizzare i requisiti di legge e/o rischi di cybersicurezza • Redazione e compilazione di quanto specificato in norma sul portale ACN.	A titolo esemplificativo e non esaustivo: • Mappatura requisiti di sicurezza Legge 90 • Report di monitoraggio aderenza a Legge 90 • Set documentali in ambito Cybersecurity per le tematiche richieste da Legge 90 • Informazioni e report da comunicare ad ACN tramite portale (Asset etc.)
dal 2026 al 2028	**S13-3 – Supporto all'indirizzo strategico, programmatico, tecnico, organizzativo, procedurale ed operativo della Cybersec di ASL Roma 1**	Servizio continuativo strategico e gestionale in ambito cybersecurity e compliance normativa e comprensivo delle seguenti attività (esemplificativo non esaustivo): • Supporto al continuo miglioramento dei macro-processi di controllo e verifica della cybersicurezza e dell'efficienza operativa degli elettromedicali in ambienti Multi/Hybri-Cloud e IoMT di ASL Roma 1 in continuità con le attività descritte per il 2025 (eg: integrazione nuovi fonti, aggiunta nuovi KPI, revisione Dashboard, ecc.) • Indirizzo strategico: supporto nella definizione e controllo delle scelte strategiche inerenti il governo della sicurezza delle informazioni, degli indirizzi organizzativi, tecnologici e dell'approccio da adottare a fronte di nuovi paradigmi architetturali, scenari di attacco e situazioni di rischio consolidate, incluso un supporto nell'identificazione dei fabbisogni di beni e servizi in materia di IT Security; • Cyber Risk: supporto nel continuo aggiornamento della lista delle minacce cyber, delle contromisure tecniche e organizzativo-procedurali più idonee e nella valutazione degli impatti degli eventuali incidenti cyber con lo scopo di orientare e adattare le politiche di sicurezza e le eventuali evoluzioni tecnologiche da adottare nel contesto aziendale. In questo contesto sono comprese anche la definizione di programmi di monitoraggio del rischio dei fornitori oltre a programmi di monitoraggio interni atti a garantire che i controlli di sicurezza delle informazioni messi in atto siano governate e operino in modo appropriato. • Validazioni tecniche e sulle attività di Security Operations: supporto ed indirizzo sui piani di rimedio derivanti dall'esecuzione di scansioni di vulnerabilità,	A titolo esemplificativo e non esaustivo: • Aggiornamento elenco nuove fonti per alimentare i KPI di cybersicurezza • Aggiornamento documentazione tecnica del data Lake di raccolta dati • Aggiornamento metodologia correlazione eventi • Formalizzazione e/o aggiornamento nuovi KPI di sicurezza e di efficienza operativa • Aggiornamento specifiche tecniche per visualizzazione KPI su sistemi di dashboarding e/o di Business Intelligence • PMO per nuovi progetti inerenti la cybersecurity (SAL e Report sulle progettualità cyber). • Piani Tattici e strategici di Cybersecurity e Data Protection • Set documentali in ambito Cybersecurity per le tematiche richieste

		di penetration test, di valutazioni della sicurezza delle applicazioni e di altre attività tecniche analoghe comprese quelle relative alla verifica che le configurazioni software e hardware presenti nel sistema informativo nell'organizzazione siano conformi a standard riconosciuti. Analisi e continua verifica che le pratiche operative di Sicurezza adottate a livello aziendale siano conformi agli standard riconosciuti di gestione della cyber sicurezza; • Internal & External Communication: supporto al collegamento cyber tra le varie unità operative dell'Ente, le terze parti interessate e nei rapporti con i fornitori, gli altri stakeholder coinvolti e le authority (es: ACN). Monitoraggio e controllo dei membri dei gruppi di lavoro che parteciperanno all'erogazione di servizi cyber. Segnalazione dei principali eventi riguardanti la sicurezza informatica sia alla Direzione IT che, nei casi più gravi ed opportuni, anche alla Direzione strategica e alle Autorità preposte. • Supporto su temi di compliance normativa in termini di: ○ Redazione e compilazione di quanto specificato in norma sul portale ACN ○ Monitoraggio e reporting (PMO) nelle attività legate alla conformità NIS2/D.Lgs 138/4 e Legge 90/2024 ○ Analisi delle implicazioni per ASL Roma 1 derivanti dalla NIS2/D.Lgs 138/24 e Legge 90/2024 e sue evoluzioni ○ Supporto e consulenza per l'attivazione presidi tecnologici ed organizzativo-procedurali utili ad indirizzare i requisiti di legge e/o rischi di cyber sicurezza	• Report e presentazioni su indirizzi strategici, rischi cyber, valutazioni tecniche e sui presidi organizzativi e procedurali della sicurezza, su metodologie e buone pratiche di Security Operations e per le comunicazioni a tutti gli stakeholder interni ed esterni. • Mappatura requisiti di sicurezza D.Lgs 138/24 e Legge 90 • Report di monitoraggio aderenza a Legge 90 • Set documentali in ambito Cybersecurity per le tematiche richieste (Cyber) NIS2/D.Lgs 138/24 e Legge 90/2024 • Raccolta informazioni e report da comunicare ad ACN tramite portale (Asset etc.)

4.1.1.2 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.

4.1.1.3 Attivazione e durata

Si prevede l'avvio del servizio entro il Q2 2025 per una durata di 48 mesi.

4.2 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 Referente NIS2/CISO.

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

4.3 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.

5 Elementi quantitativi e qualitativi per il dimensionamento servizi

5.1 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	Numero Key user coinvolti
Anno 2025			
L2.S16	Security Strategy	**1600**	< 10
Anno 2026			
L2.S16	Security Strategy	**1600**	< 10
Anno 2027			
L2.S16	Security Strategy	**1600**	< 10
Anno 2028			
L2.S16	Security Strategy	**1600**	< 10

5.2 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.

5.3 Pianificazione dei servizi

La durata ipotizzata per la fornitura è di 48 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 2025				Anno 2026				Anno 2027				Anno 2028				Anno 2029			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
L2.S16																				

Identificativo: Piano Operativo - Cybersecurity Re-Enforcement – ASL Roma 1

Data: 20/03/2025

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 – Cybersecurity Re-Enforcement

ASL Roma 1

Costituito

Raggruppamento Temporaneo di Imprese

composto da:

Deloitte Consulting S.r.l. S.B.

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 Consulting S.r.l. S.B. 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, originariamente di 24 mesi, è stata estesa a 35 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 Operativo" (o "Ordinativo di fornitura"), nel quale l'RTI intende formulare la proposta tecnico/economica secondo le modalità tecniche ed i listini previsti nell'Accordo Quadro.

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****;*

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/ACRONNIMO	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 PA	
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
	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

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:

- Attuazione di un processo di "Cybersecurity Re-Enforcement" relativa alle attività di Cloud Migration di alcuni servizi IT erogati dall'ASL Roma 1;
- Definizione e consolidamento KPI di Cybersicurezza negli ambienti Multi/Hybrid-Cloud e dell'efficienza operativa legata ai Medical Device;
- Mantenimento del sistema di conformità a Leggi e Regolamenti (es: D.Lgs 138/2024, Legge 90/24, GDPR, ecc;

4.2 Servizi richiesti

SERVIZI RICHIESTI				
ID	**NOME SERVIZIO**	**VOCE DI COSTO**	**QUANTITA'** (gg Team ottimale)	**IMPORTO** (Esente IVA)
Anno 2025				
L2.S16 – Security Strategy	**S16 – 1** Supporto nell'evoluzione e nell'integrazione dei processi operativi relativi al monitoraggio dei livelli di sicurezza e dei livelli di efficienza operativa dei medical device negli ambienti Multi/Hybri-Cloud e IoMT di ASL Roma 1	L2.S16 — gg/p Team ottimale	**1200**	**300.000 €**
L2.S16 – Security Strategy	**S16 – 2** Supporto su tematiche di Conformità Normativa (*Legge 90/2024*) e su esigenze amministrative verso ACN	L2.S16 — gg/p Team ottimale	**400**	**100.000 €**
Anno 2026				
L2.S16 – Security Strategy	**S16 – 3** Supporto all'indirizzo strategico, programmatico, tecnico, organizzativo, procedurale ed operativo della Cybersecurity e della Conformità Normativa (*NIS2/D.Lgs 138/24 - Legge 90/2024*)	L2.S16 — gg/p Team ottimale	**1600**	**400.000 €**
Anno 2027				
L2.S16 – Security Strategy	**S16 – 3** Supporto all'indirizzo strategico, programmatico, tecnico, organizzativo, procedurale ed operativo della Cybersecurity e della Conformità Normativa (*NIS2/D.Lgs 138/24 - Legge 90/2024*)	L2.S16 — gg/p Team ottimale	**1600**	**400.000 €**
Anno 2028				
L2.S16 – Security Strategy	**S16 – 3** Supporto all'indirizzo strategico, programmatico, tecnico, organizzativo, procedurale ed operativo della Cybersecurity e della Conformità Normativa (*NIS2/D.Lgs 138/24 - Legge 90/2024*)	L2.S16 — gg/p Team ottimale	**1600**	**400.000 €**
			TOTALE (Esclusa IVA)	**1.600.000 €**

4.3 Dettaglio dei servizi richiesti

4.3.1 L2.S16 - Security Strategy

4.3.1.1 Descrizione e caratteristiche del servizio

Anni	Attività	Dettagli sulle attività	Deliverable
2025	S16-1 – Supporto nell'evoluzione e nell'integrazione dei processi operativi relativi al monitoraggio dei livelli di sicurezza e dei livelli di efficienza operativa dei medical device negli ambienti Multi/Hybri-Cloud e IoMT di ASL Roma 1	Le attività in questione hanno il fine di supportare il miglioramento continuo dei macro-processi di controllo e verifica della cybersicurezza e dell'efficienza operativa degli elettromedicali in ambienti Multi/Hybri-Cloud e IoMT di ASL Roma 1. Il servizio si esplicita nella serie di attività elencate qui di seguito: • Identificazione di tutte le fonti che possono concorrere ad alimentare il Data Lake di ASL Roma 1 e che possono essere utili all'evoluzione delle dashboard di cybersecurity e di efficienza operativa; • Ingegnerizzazione del sistema di raccolta ed elaborazione dei dati nel Data Lake anche in funzione di possibili integrazioni con altri sistemi di Business Intelligence già in fase di sviluppo presso ASL Roma 1. Nota: allo stato attuale il Data Lake raccoglie dati dalle seguenti fonti: ○ Claroty xDome (ex Medigate) ○ Security View (Asset Inventory + risultanze VAPT) ○ Web Application Firewall (WAF) ○ Moduli Fortinet (Firewall, Multi Factor Autentication, Priviledge Account Management, Network Access Control) • Definizione e sviluppo della metodologia di correlazione degli eventi, funzionale allo sviluppo di KPI/reporting di supporto alle decisioni • Armonizzazione col sistema di VAPT ampliato ai medical device sul perimetro cyber • Supporto alla definizione delle specifiche tecniche utili alla visualizzazione dei KPI di Cybersecurity e di efficienza operativa dei dispositivi elettromedicali (per successive implementazioni su sistemi di dashboarding/reporting esistenti o eventuali sistemi di Business Intelligence in uso/futuri) • Integrazione di Dashboard utili a rappresentare l'andamento di un max di ulteriori 20 KPI rispetto alle attuali.	• Elenco nuove fonti • Descrizione del data Lake di raccolta dati • Metodologia correlazione eventi • Formalizzazione e/o aggiornamento nuovi KPI di sicurezza e di efficienza operativa (c.ca 50) • Specifiche tecniche per visualizzazione KPI su sistemi di dashboarding e/o di Business Intelligence • Dashboard per ulteriori 20 KPI.

Anni	Attività	Dettagli sulle attività	Deliverable
2025	S16-2 – Supporto su tematiche di Conformità Normativa (Legge 90/2024) e su esigenze amministrative verso ACN	Servizio continuativo strategico e gestionale comprensivo delle seguenti attività: • Monitoraggio e reporting (PMO) nelle attività legate alla conformità Legge 90/2024 • Analisi delle implicazioni per ASL Roma 1 derivanti dalla Legge 90/2024 e sue evoluzioni • Supporto e consulenza relativamente alla eventuale attivazione di presidi tecnologici ed organizzativo-procedurali utili ad indirizzare i requisiti di legge e/o rischi di cybersicurezza • Redazione e compilazione di quanto specificato in norma sul portale ACN.	A titolo esemplificativo e non esaustivo: • Mappatura requisiti di sicurezza Legge 90 • Report di monitoraggio aderenza a Legge 90 • Set documentali in ambito Cybersecurity per le tematiche richieste da Legge 90 • Informazioni e report da comunicare ad ACN tramite portale (Asset etc.)
dal 2026 al 2028	S13-3 – Supporto all' indirizzo strategico, programmatico, tecnico, organizzativo, procedurale ed operativo della Cybersec di ASL Roma 1	Servizio continuativo strategico e gestionale in ambito cybersecurity e compliance normativa e comprensivo delle seguenti attività (esemplificativo non esaustivo): • Supporto al continuo miglioramento dei macro-processi di controllo e verifica della cybersicurezza e dell'efficienza operativa degli elettromedicali in ambienti Multi/Hybri-Cloud e IoMT di ASL Roma 1 in continuità con le attività descritte per il 2025 (eg: integrazione nuovi fonti, aggiunta nuovi KPI, revisione Dashboard, ecc.) • Indirizzo strategico: supporto nella definizione e controllo delle scelte strategiche inerenti il governo della sicurezza delle informazioni, degli indirizzi organizzativi, tecnologici e dell'approccio da adottare a fronte di nuovi paradigmi architetturali, scenari di attacco e situazioni di rischio consolidate, incluso un supporto nell'identificazione dei fabbisogni di beni e servizi in materia di IT Security; • Cyber Risk: supporto nel continuo aggiornamento della lista delle minacce cyber, delle contromisure tecniche e organizzativo-procedurali più idonee e nella valutazione degli impatti degli eventuali incidenti cyber con lo scopo di orientare e adattare le politiche di sicurezza e le eventuali evoluzioni tecnologiche da adottare nel contesto aziendale. In questo contesto sono comprese anche la definizione di programmi di monitoraggio del rischio dei fornitori oltre a programmi di monitoraggio interni atti a garantire che i controlli di sicurezza delle	A titolo esemplificativo e non esaustivo: • Aggiornamento elenco nuove fonti per alimentare i KPI di cybersicurezza • Aggiornamento documentazione tecnica del data Lake di raccolta dati • Aggiornamento metodologia correlazione eventi • Formalizzazione e/o aggiornamento nuovi KPI di sicurezza e di efficienza operativa • Aggiornamento specifiche tecniche per visualizzazione KPI su sistemi di dashboarding e/o di Business Intelligence • PMO per nuovi progetti inerenti la cybersecurity (SAL e Report sulle progettualità cyber). • Piani Tattici e strategici di Cybersecurity e Data Protection

Anni	Attività	Dettagli sulle attività	Deliverable
		informazioni messi in atto siano governate e operino in modo appropriato. • Validazioni tecniche e sulle attività di Security Operations: supporto ed indirizzo sui piani di rimedio derivanti dall'esecuzione di scansioni di vulnerabilità, di penetration test, di valutazioni della sicurezza delle applicazioni e di altre attività tecniche analoghe comprese quelle relative alla verifica che le configurazioni software e hardware presenti nel sistema informativo nell'organizzazione siano conformi a standard riconosciuti. Analisi e continua verifica che le pratiche operative di Sicurezza adottate a livello aziendale siano conformi agli standard riconosciuti di gestione della cyber sicurezza; • Internal & External Communication: supporto al collegamento cyber tra le varie unità operative dell'Ente, le terze parti interessate e nei rapporti con i fornitori, gli altri stakeholder coinvolti e le authority (es: ACN). Monitoraggio e controllo dei membri dei gruppi di lavoro che parteciperanno all'erogazione di servizi cyber. Segnalazione dei principali eventi riguardanti la sicurezza informatica sia alla Direzione IT che, nei casi più gravi ed opportuni, anche alla Direzione strategica e alle Autorità preposte. • Supporto su temi di compliance normativa in termini di: ○ Redazione e compilazione di quanto specificato in norma sul portale ACN ○ Monitoraggio e reporting (PMO) nelle attività legate alla conformità NIS2/D.Lgs 138/4 e Legge 90/2024 ○ Analisi delle implicazioni per ASL Roma 1 derivanti dalla NIS2/D.Lgs 138/24 e Legge 90/2024 e sue evoluzioni ○ Supporto e consulenza per l'attivazione presidi tecnologici ed organizzativo-procedurali utili ad indirizzare i requisiti di legge e/o rischi di cyber sicurezza	• Set documentali in ambito Cybersecurity per le tematiche richieste • Report e presentazioni su indirizzi strategici, rischi cyber, valutazioni tecniche e sui presidi organizzativi e procedurali della sicurezza, su metodologie e buone pratiche di Security Operations e per le comunicazioni a tutti gli stakeholder interni ed esterni. • Mappatura requisiti di sicurezza D.Lgs 138/24 e Legge 90 • Report di monitoraggio aderenza a Legge 90 • Set documentali in ambito Cybersecurity per le tematiche richieste (Cyber) NIS2/D.Lgs 138/24 e Legge 90/2024 • Raccolta informazioni e report da comunicare ad ACN tramite portale (Asset etc.)

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 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 saranno erogate presso le sedi dell'Amministrazione Contraente /da remoto (presso le sedi del RTI, o presso altra sede da concordare con l'Amministrazione Stessa.

4.3.1.3 Attivazione e durata

Si prevede l'avvio del servizio entro il Q2 2025 per una durata di 48 mesi.

4.4 Indicatori di digitalizzazione

Nell'ambito delle attività di governance ed in particolare della valutazione del livello di efficacia degli interventi operati dalle Amministrazioni attraverso l'utilizzo di contratti esecutivi afferenti alle Gare Strategiche in ambito Sicurezza ICT, si intendono definite due tipologie di indicatori:

- **Indicatori Generali**, che mappano il macro-obiettivo dell'intervento rispetto ai principali obiettivi strategici del Piano Triennale;
- **Indicatori Specifici**, che definiscono, sulla base delle specificità della Gara Strategica, le misure di digitalizzazione applicabili allo specifico contratto esecutivo, in funzione dei prodotti/servizi acquisiti. In tale contesto, è definito un indicatore (cd. "indicatore di progresso" in seguito descritto) che indica il livello di maturità della infrastruttura di sicurezza ICT delle Amministrazioni, sulla base del grado di mappatura degli interventi effettuati con le misure minime di sicurezza AGID (Circolare 18 aprile 2017, n. 2/2017, Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)»).

Gli indicatori saranno utilizzati per il monitoraggio dei contratti e del raggiungimento dei relativi obiettivi.

Nel contesto AQP, per la tipologia di interventi previsti, si considerano gli indicatori presentati nei prossimi due paragrafi e che saranno oggetto di monitoraggio nell'intero arco temporale dell'incarico presentato in questo Piano Operativo.

4.4.1 Indicatori generali di digitalizzazione

Di seguito si riportano gli indicatori Generali di digitalizzazione previsti per la presente fornitura:

	INDICATORI DI COLLABORAZIONE E RIUSO	VALORE EX ANTE	VALORE EX POST
1	**Riuso di processi per erogazione servizi digitali**	*Nessuna*	*Gestione Uniforme della Sicurezza delle informazioni per i servizi erogati dai Datacenter di AQP* *Dato da valorizzare ogni 12 mesi*

Per ciascuno dei sopra riportati indicatori, verrà effettuata una valutazione in fase di avvio degli interventi progettuali e a valle (ogni 12 mesi), così da misurare il livello di digitalizzazione raggiunto per ciascuno di essi.

4.4.2 Indicatori di progresso

Per ogni classe di controlli ABSC (Agid Basic Security Control) previsti dalle misure minime di sicurezza AGID, ove successivamente modificate ed integrate, sarà calcolato il valore del relativo Indicatore di Progresso (Ip) dell'intervento ottenuto attraverso la realizzazione dell'Ordinativo di Fornitura (acquisto di servizi previsti nell'Ordinativo), che sarà determinato come da schema seguente:

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

Lo studio della effettiva applicabilità e la conseguente scelta e valorizzazione ex-ante ed ex-post degli indicatori di progresso è una delle attività previste in questo Piano Operativo all'interno dei servizi afferenti al L2.S16 – Security Strategy.

5 Organizzazione e modalità di erogazione del contratto esecutivo

5.1 Attività in carico alle aziende del RTI

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

SERVIZIO	Deloitte Consulting	EY Advisory	Teleco
L2.S16	75,00%	25,00%	0%
TOTALE	**75,00%**	**25,00%**	**0%**

5.2 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	[redacted]
Referente Tecnico CE (RT)	
Responsabile Attività L2.S16	

5.3 Modalità di esecuzione dei servizi

Le attività relative all'esecuzione dei servizi saranno erogate presso le sedi dell'Amministrazione Contraente o da remoto.

6 Piano di lavoro

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	Numero Key user coinvolti
Anno 2025			
L2.S16	Security Strategy	**1600**	< 10
Anno 2026			
L2.S16	Security Strategy	**1600**	< 10
Anno 2027			
L2.S16	Security Strategy	**1600**	< 10
Anno 2028			
L2.S16	Security Strategy	**1600**	< 10

6.2 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	W1	W2	W3	W4	W5
Pianificazione	Pianificazione delle attività					
Predisposizione Strumenti	Predisposizione e aggiornamento strumenti					
Assessment documentale	Analisi AS IS dei progetti in corso					
Acquisizione competenze	Incontri con il personale dell'Amministrazione, training on the job, self training, workshop					
Ottimizzazione	Individuazione delle possibili aree di miglioramento					
Fine presa in carico	Ricognizione e verifica delle attività svolte					
Governance	Verifica dello stato delle attività					

6.3 Cronoprogramma

La durata ipotizzata per la fornitura è di 48 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.

Obiettivi/Servizi	Anno 2025				Anno 2026				Anno 2027				Anno 2028				Anno 2029			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
L2.S16																				

6.4 Data di attivazione e durata del servizio

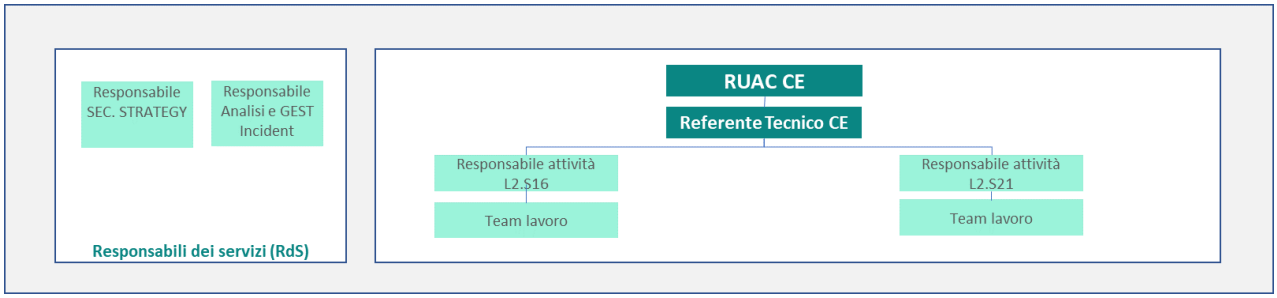
Il contratto esecutivo avrà i suoi effetti dalla data di stipula e avrà una durata di **48 mesi** dalla data di attivazione dei servizi, compatibilmente con il vincolo definito dall'Accordo quadro, ovvero che i Contratti Esecutivi abbiano una durata massima pari alla durata residua, al momento della sua stipula, dell'Accordo Quadro.

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



Nei successivi paragrafi sono declinate le figure previste all'interno del Team di Lavoro di ciascun servizio.

Security Strategy (L2.S16)

Il team ottimale sarà composto dalle seguenti figure con le relative responsabilità assegnate:

Profilo	Responsabilità
Security Principal	Project Manager, ha lo scopo di definire e gestire il progetto dal concepimento iniziale alla consegna finale. Responsabile dell'ottenimento di risultati ottimali, conformi agli standard di qualità, sicurezza e sostenibilità nonché coerenti con gli obiettivi, le performance, i costi ed i tempi definiti.
Security Solution Architect	Figura professionale dedicata al mantenimento della sicurezza del sistema informatico di un'organizzazione. Sarà responsabile dell'analisi dell'infrastruttura IT e delle relazioni tra i differenti sistemi e componenti infrastrutturali volta all'individuazione di problematiche architetturali che ne potrebbero compromettere la sicurezza. Si occuperà, inoltre, dell'analisi delle configurazioni e delle regole tecniche delle principali soluzioni di sicurezza utilizzate per proteggere l'infrastruttura e i servizi (Firewall, IPS/IDS, SIEM, soluzioni anti-malware,

	Web Application Firewall, Database Monitoring, servizi Anti-DDoS, servizi cloud oriented per la sicurezza).
Senior Information Security Consultant	Presidia l'attuazione della strategia definita all'interno del suo ambito di responsabilità (sia questo un progetto, un processo, una location) coordinando attivamente le eventuali figure operative a lui assegnate per tale scopo, rappresentando il naturale raccordo tra la struttura di governance della cyber security e il resto del personale operativo. Controlla il rispetto alle regole definite e del cogente in materia di sicurezza delle informazioni. Pianifica ed attua misure di sicurezza per proteggere le reti e i sistemi informatici di un'organizzazione.
Senior Security Auditor	Garantisce la conformità con le procedure di controllo interno stabilite esaminando i registri, i rapporti, le pratiche operative e la documentazione. Completa i giornali di audit documentando test e risultati dell'audit. Individua i possibili punti vulnerabili di un sistema informativo.
Data Protection Specialist	Esperto nella protezione dei dati personali e dotato di competenze giuridiche e informatiche specifiche, verifica il rispetto di quanto previsto nelle normative italiane ed europee in termini di protezione dei dati nonché delle politiche applicate dal titolare del trattamento o dal responsabile del trattamento in materia di protezione dei dati personali

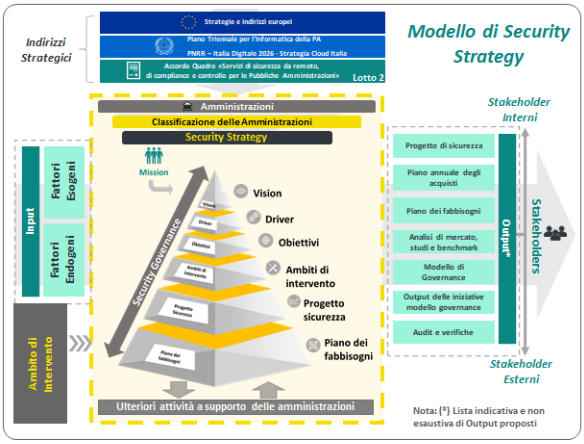
Il RTI si impegna a modificare o ampliare la composizione del team di progetto in funzione dell'operatività e dei deliverable richiesti, garantendo la disponibilità dei profili professionali e delle competenze previste.

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.