Identificativo: ARPA Piemonte_Piano Operativo v. 1.0.

Data: 04/04/2025

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

ARPA Piemonte

Costituito

Raggruppamento Temporaneo di Imprese

composto da:

Deloitte Consulting S.r.l. SB

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. SB 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 e poi 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

Nell'ambito dell'Accordo Quadro per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni (Sigef 2296, Lotto2), ARPA Piemonte intende acquisire la fornitura di alcuni servizi da Deloitte per attuare interventi volti ad innalzare il livello di maturità dell'Amministrazione in ambito cyber**.** Gli interventi avverranno nell'ambito dell'Avviso 8/2024 dell'Agenzia per la Cybersicurezza Nazionale, promosso per l'attuazione degli investimenti finalizzati alla realizzazione di interventi di potenziamento della resilienza cyber per la Pubblica Amministrazione. Nello specifico trattasi dei servizi che ricadano sotto i seguenti categorie:

- **Servizio L2.S16 – Security Strategy**
- **Servizio L2.S22 – Penetration Test**

Si veda inoltre la sezione 4 e successive sotto-sezioni per un dettaglio dei servizi richiesti.

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
CE	Contratto Esecutivo
PAL	Pubblica Amministrazione Locale

2 Anagrafica dell'amministrazione

DATI ANAGRAFICI DELL'AMMINISTRAZIONE	
Ragione sociale Amministrazione	Agenzia regionale per la protezione ambientale del Piemonte (ARPA Piemonte)
Indirizzo	Via Pio VII 9
CAP	10135
Comune	Torino
Provincia	Torino (TO)
Regione	Piemonte
Codice Fiscale	07176380017
Indirizzo mail	direzionegenerale@arpa.piemonte.it
PEC	protocollo@pec.arpa.piemonte.it
Codice PA	arlpa_to
Comparto di Appartenenza (PAL/PAC)	PAL

DATI ANAGRAFICI REFERENTE DELL'AMMINISTRAZIONE	
Nome	Diego
Cognome	Rullo
Telefono	01119680111
Indirizzo mail	dip.coordinamento.servizi@arpa.piemonte.it
PEC	protocollo@pec.arpa.piemonte.it

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

La crescente e profonda evoluzione delle minacce informatiche nel contesto della pubblica amministrazione ha reso imperativo adottare una serie di misure di sicurezza cibernetica altamente sofisticate, mirate a contrastare e mitigare tali minacce. In questo contesto, diventa essenziale porre una maggiore attenzione sulle tematiche relative alla sicurezza delle informazioni e alla protezione dei dati sensibili.

Per far fronte a questa sfida in rapida evoluzione, ARPA Piemonte ha riconosciuto l'urgente necessità di potenziare e irrobustire i propri processi, sistemi e servizi. Questo obiettivo si pone al centro delle strategie dell'ente, con l'obiettivo di garantire un ambiente digitale sicuro e resiliente con l'obiettivo di migliorare globalmente la qualità e l'affidabilità dei servizi informativi offerti dall'Ente.

La protezione delle informazioni sensibili e la sicurezza dei dati diventano, quindi, aspetti fondamentali nell'ottica di costruire una solida postura di sicurezza cibernetica. Ciò richiede un approccio olistico e proattivo, dove la consapevolezza dei rischi e l'implementazione di migliori pratiche di cybersecurity si combinano per formare una barriera di difesa contro le minacce in costante evoluzione.

In linea con quanto descritto in precedenza sono stati individuati, nell'ambito del Lotto 2 – Servizi di Compliance e controllo dell'Accordo Quadro, avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni, al fine di innalzare il livello di maturità cyber dell'amministrazione, una serie di servizi attraverso l'esecuzione di attività in ambito **Security Strategy (L2.S16)** e **Penetration Test (L2.S22)** che perseguono i seguenti obiettivi:

- **Obiettivo 1:** Definire il **livello di maturità cyber** di ARPA Piemonte, attraverso lo svolgimento di un'attività di cyber security posture assessment e conseguente definizione di un piano di potenziamento, in relazione all'avvio di un processo di certificazione ISO 27001:2022;
- **Obiettivo 2:** Definizione delle **principali policy e procedure** funzionali a garantire una governance efficace dei processi di cybersicurezza, in linea con i requisiti previsti dallo standard ISO 27001:2022;
- **Obiettivo 3:** Definire il livello di maturità sulle **tematiche Privacy** di ARPA Piemonte, attraverso lo svolgimento di un'attività verticale di assessment e conseguente definizione di un piano di potenziamento;
- **Obiettivo 4:** Definizione ed erogazione di **programmi di awareness, formazione** in ambito cybersecurity, personalizzata per target di utenti, volta ad innalzare il livello di consapevolezza del personale
- **Obiettivo 5:** Esecuzione di un **Cyber Risk Assessment** per la valutazione del rischio informatico legato all'infrastruttura IT dell'Ente, finalizzato all'individuazione, classificazione e valutazione dei rischi e delle minacce informatiche
- **Obiettivo 6:** definizione di un **framework documentale** di cybersicurezza in ambito **Incident ed Event Management** funzionale a garantire una gestione efficace e una risposta tempestiva agli eventi e/o incidenti di cybersicurezza.
- **Obiettivo 7:** Stesura di un framework documentale in ambito **Business Continuity** e di **Crisis Management** funzionale a garantire la resilienza dell'Ente di fronte ad eventi avversi
- **Obiettivo 8:** Attività di **Penetration Testing** per individuare eventuali falle e vulnerabilità nei sistemi, consentendo così di testare e sviluppare le necessarie azioni correttive.

4.2 Servizi richiesti

4.3 Dettaglio dei servizi richiesti

SERVIZI RICHIESTI				
Servizio	**NOME SERVIZIO**	**VOCE DI COSTO**	**QUANTITA' (gg/p Team ottimale)**	**IMPORTO (IVA esclusa)**
L2.S16 – Security Strategy	1. Esecuzione di un Cybersecurity Posture e ISO Readiness Assessment	gg/p Team ottimale	360	90.000,00 €
	2. Stesura di una framework documentale in ambito cybersecurity	gg/p Team ottimale	368	92.000,00 €
	3. Esecuzione di un assessment verticale sulle normative privacy	gg/p Team ottimale	200	50.000,00 €
	4. Formazione in ambito cybersecurity	gg/p Team ottimale	352	88.000,00 €
	5. Esecuzione di un Cyber Risk Assessment	gg/p Team ottimale	280	70.000,00 €
	6. Stesura di un framework documentale in ambito Incident & Event Management	gg/p Team ottimale	200	50.000,00 €
	7. Stesura di un framework documentale in ambito Business Continuity e di Crisis Management	gg/p Team ottimale	720	180.000,00 €
L2.S22 Penetration Testing	8. Attività di Penetration Testing	gg/p Team ottimale	485	80.025,00 €
TOTALI			**2.965**	**700.025,00 €**

4.3.1 L2.S16 - Security Strategy

4.3.1.1 Descrizione e caratteristiche del servizio

Macro-attività	Attività	Deliverable
1. Esecuzione di un Cybersecurity Posture e ISO Readiness Assessment	L'intervento prevede un'analisi del contesto operativo attuale al fine di valutare lo stato di maturità cyber dell'Amministrazione in relazione all'avvio di un processo di certificazione ISO 27001:2022. L'attività prevede: • Valutazione dei livelli di maturità in termini di processi, organizzazione e tecnologie rispetto al Framework Nazionale per la Cybersecurity e la Data Protection e dei requisiti della norma ISO 27001:2022 • Definizione dei livelli di maturità desiderati • Predisposizione di una Gap Analysis • Predisposizione del Remediation Plan	• Presentazione di avvio progetto • Documento di checklist diagnostica • Documento contenente i risultati dell'Assessment e di analisi delle aree di scopertura • Piano di Rimedio per gli interventi prioritari individuati • Presentazione dei risultati
2. Stesura di una framework documentale in ambito cybersecurity	L'intervento prevede la definizione delle principali policy e procedure funzionali a garantire una governance efficace dei processi di cybersicurezza, in linea con i requisiti previsti dallo standard ISO 27001:2022, i principali obblighi normativi e standard di settore applicabili. Un input all'attività sarà inoltre dato dalla fase precedente di assessment, che permetterà di indentificare i documenti da mettere in priorità, rispetto a quanto già in essere presso l'Ente.	6 tra politiche e procedure che saranno identificate nella fase di assesssment, tra cui a titolo di esempio: • Politica generale di sicurezza delle informazioni • Procedura gestione delle vulnerabilità • Procedura Gestione degli Asset • Guida all'utilizzo degli strumenti e risorse informatiche • Procedura Gestione dei Log • Linee guida/procedure relative alla security by design e sviluppo sicuro
3. Esecuzione di un assessment verticale sulle normative privacy	L'intervento prevede un'attività di assessment verticale sulle normative privacy in cui, oltre al Regolamento GDPR e regolamentazione nazionale, saranno inclusi i Provvedimenti dell'Autorità Garante e il Framework privacy dell'Ente, in linea con i requisiti richiesti dallo standard ISO 27001:2022.	• Documento contenente i risultati dell'Assessment e di analisi delle aree di scopertura • Piano di Rimedio per gli interventi prioritari individuati • Presentazione dei risultati

Macro-attività	Attività	Deliverable
4. Formazione in ambito cybersecurity	L'intervento prevede la definizione ed erogazione di programmi di awareness, formazione in ambito cybersecurity, personalizzata per target di utenti. In particolare, le attività prevederanno: • Formazione base: Workshop di cybersecurity • Formazione avanzata: Phishing Campaigns e Simulazioni TableTop	• Presentazioni utilizzate durante il workshop. • Piano di Campagna Phishing • Report di Risultati della Campagna Phishing • Documento contenente gli scenari simulati nell'esercitazioni TableTop, ruoli e responsabilità assegnati ai partecipanti • Report dei Risultati della Simulazione TableTop
5. Esecuzione di un Cyber Risk Assessment	L'intervento prevede l'esecuzione di un Cyber Risk Assessment per la valutazione del rischio informatico legato all'infrastruttura IT dell'Ente, finalizzato all'individuazione, classificazione e valutazione dei rischi e delle minacce informatiche. In particolare, l'attività comprende: • Definizione del perimetro dell'attività e individuazione degli asset e processi critici • Identificazione e valutazione delle minacce e vulnerabilità cyber attraverso un approccio statico o dinamico sul perimetro di riferimento e successiva classificazione in base a criteri come la probabilità di accadimento, l'impatto sull'amministrazione a livello operativo o funzionale e presenza di contromisure efficaci • Sviluppo di strategie, misure di sicurezza e piani di trattamento dei rischi identificati, in modo da implementare iniziative efficaci per trasferirlo, mitigarlo e/o accettarlo (es. tramite l'adozione di policy e/o procedure)	• Presentazione di avvio progetto e Piano delle attività • Documento di descrizione della metodologia e delle fasi adottate. • Documento contenente i risultati dell'Assessment, inclusi i principali rischi e le raccomandazioni. • Presentazione di alto livello dei Risultati dell'Assessment
6. Stesura di un framework documentale in ambito Incident & Event Management	L'intervento prevede la stesura di una o più policy e procedure funzionali a garantire una gestione efficace e una risposta tempestiva agli incidenti di sicurezza e un piano di ripristino da attuare in caso di incidente. L'obiettivo è definire ruoli e responsabilità, metodologie di classificazione degli eventi, tempi, valutazione degli impatti e soglie che devono essere superate per classificare l'evento come incidente. Si prevede la definizione e formalizzazione, inoltre, del processo di gestione delle comunicazioni da effettuarsi a seguito di incidenti di cybersecurity, in termini di flussi comunicativi sia interni che esterni.	• Procedura di Incident Management

Macro-attività	Attività	Deliverable
7. Stesura di un framework documentale in ambito Business Continuity e il Crisis Management	L'attività prevederà la stesura di un framework documentale in ambito Business Continuity e il Crisis Management che permetta all'Ente di far fronte ad incidenti o crisi che possano a mettere a rischio l'operatività dell'Ente, permettendo di innalzare il livello di resilienza dell'Ente e allineato ai principali standard di settore, quali ISO 22301:2019 e ISO 22361:2022.	• Piano di Continuità Operativa • Procedura di Crisis Management

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 delle attività e degli elaborati finali, dimensionati e valorizzati economicamente. La consuntivazione avverrà sulla base dello stato dell'avanzamento lavori (SAL) bimestrale determinato coerentemente con il piano di lavoro definito.

Il gruppo 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 e da remoto (es: presso le sedi del RTI).

4.3.1.3 Attivazione e durata

Si richiede la disponibilità per l'avvio del servizio entro il **Q2 2025** e fino al **Q4 2025,** per una durata di circa 9 mesi

4.3.2 L2.S22 - Penetration testing

Il servizio fornisce alle Amministrazioni un processo operativo di analisi e valutazione dei punti deboli relativi ad una infrastruttura IT.

Il servizio, condotto su più fasi e mediante l'adozione di adeguati strumenti, si configura nella simulazione di un attacco informatico al sistema da parte di un utente malintenzionato al fine di rilevare la presenza di eventuali falle e vulnerabilità al suo interno. Il servizio fornisce il maggior numero di informazioni sulle vulnerabilità che hanno permesso l'accesso non autorizzato al sistema con una stima chiara sulle capacità di difesa e sul livello di penetrazione raggiunto.

Come già concordato con l'Amministrazione, il servizio verrà eseguito per le Applicazioni/Moduli, nella seguente modalità:

- **Gray Box**: il test presuppone conoscenze e informazioni parziali, tra cui le credenziali di accesso e profili applicativi.

Inoltre, per permettere una corretta quantificazione del servizio, le Applicazioni/Moduli oggetto di analisi, sono classificati mediante il seguente criterio:

- **Light:** Applicazioni/Moduli applicativi non critici che consentono la visualizzazione di pagine di contenuto informativo (es: siti web statici) o l'utilizzo di un numero ridotto di funzionalità - Attività con massimo 1 profilo applicativo.
- **Small:** Applicazioni/Moduli applicativi che consentono la visualizzazione di una modesta quantità di pagine dinamiche e funzionalità (URL/parametri) - Attività con massimo 2 profili applicativi.
- **Medium:** PT Applicazioni/Moduli applicativi costituiti da più form (siti web dinamici, APIs, Web Services ecc.) e con funzionalità di autenticazione complesse (es MFA) - Attività con massimo 2 profili applicativi.
- **Large:** PT Applicazioni/Moduli applicativi critici con funzionalità complesse e di tipo transazionale (ad esempio pagamenti) - Attività con massimo 2 profili applicativi.

4.3.2.1 Descrizione e caratteristiche del servizio

Macro-attività	Attività	Deliverable
Penetration Test	• **Penetration Test Applicativo** di tipo Grey Box, su un totale di **8** applicazioni. Di seguito il dettaglio: ○ **Target:** • **2 Light:** ▪ Sito radar Protezione Civile ▪ Sito Rapporto Stato Ambiente • **3 Small:** ▪ modulo invio dati URP del sito Arpa Istituzionale ▪ sito Meteo3R ▪ web application "IrisAPP" • **3 Medium:** ▪ sito Geoportale ▪ sito snippets Rischi Naturali ▪ sito GAU esterno per ASL ○ **Periodicità**: 1 run	• Report dei test, comprensivo di: - Executive Summary - Dettaglio tecnico - Indicazioni di rimedio

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 del team ottimale*".

Saranno definiti di concerto con l'Amministrazione dei task e dei deliverable, dimensionati e valorizzati economicamente. La fatturazione avverrà sulla base dello stato dell'avanzamento lavori determinato coerentemente con il piano di lavoro definito alla consegna dei deliverable concordati previo benestare/e sarà riconosciuta bimestralmente.

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

4.3.2.3 Attivazione e durata

Si richiede la disponibilità per l'avvio del servizio entro il **Q2 2025** e fino al **Q4 2025,** per una durata di circa 9 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 di ARPA, 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 ARPA Piemonte.* *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 dell'effettiva applicabilità e la conseguente scelta e valorizzazione ex-ante ed ex-post degli indicatori di progresso è una delle attività che prevediamo all'interno del servizio **L2.S16 Security Strategy** e **L2.S22 Penetration Testing**.

5 Organizzazione e modalità di erogazione del contratto esecutivo

5.1 Attività in carico alle aziende del RTI

SERVIZIO	Deloitte Consulting (100%)	EY Advisory (0%)	Teleco (0%)
L2.S16	100%	0%	0%
L2.S22	100%	0%	0%
TOTALE	**100%**	**0%**	**0%**

5.2 Modalità di ricorso al subappalto da parte del fornitore

SERVIZIO	AZIENDA	QUOTA SUBAPPALTATA
L2.S16	**Deloitte Consulting Srl S.B.**	**Fino al 50%**
L2.S22	**Deloitte Consulting Srl S.B.**	**Fino al 50%**

Si precisa che la quota di subappalto della singola Società non potrà mai essere superiore alla quota massima subappaltabile fatta salva espressa deroga concessa dal Committente.

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
Referente Tecnico CE (RT)	Marco Ceccon
Responsabile Attività L2.S16	Andrea Abate
Responsabile Attività L2.S22	Michele Dell'Uomo

5.4 Modalità di esecuzione dei servizi

Le attività saranno erogate presso le sedi dell'Amministrazione Contraente e da remoto.

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	W1	W2	W3	W4
Incontri con l'Amministrazione	Incontri con il personale dell'Amministrazione volti a validare gli obiettivi di progetto e le relative modalità di esecuzione				
Predisposizione documentazione di gestione del progetto	Predisposizione degli strumenti e documentazione a supporto della gestione del progetto (presentazione di avvio attività, SAL ecc.)				
Avvio attività di PMO	Avvio delle attività di coordinamento del progetto per consentire il corretto svolgimento delle attività progettuali nelle tempistiche di progetto previste				

6.2 Cronoprogramma

La durata ipotizzata per la fornitura è di **9 mesi** dalla data di attivazione, compatibilmente con le tempistiche indicate nell'**avviso pubblico n. 08/2024** per la presentazione di proposte di interventi di potenziamento della resilienza cyber previsto dal Piano Nazionale di Ripresa e Resilienza (PNNR).

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

		Mese 1	Mese 2	Mese 3	Mese 4	Mese 5	Mese 6	Mese 7	Mese 8	Mese 9
L2.S16 Security Strategy	**1**. Cybersecurity Posture e ISO Readiness Assessment									
	2. Framework documentale in ambito cybersecurity									
	3. Assessment verticale sulle normative privacy									
	4. Formazione in ambito cybersecurity									
	5. Esecuzione di un Cyber Risk Assessment									

	6. Framework documentale Incident & Event Mgmt									
	7. Framework documentale BCM e Crisis Management									
L2.S22 Penetration Test	**8.** Attività di Penetration Testing									

6.3 Data di attivazione e durata del servizio

Le attività, compatibilmente con l'avvio del progetto entro massimo **30 giorni** dall'emissione del seguente piano e la disponibilità del personale dell'Amministrazione coinvolto nello svolgimento delle attività progettuali, si concluderanno improrogabilmente entro il **31/12/2025.**

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.

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.
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.

Penetration Test (L2.S22)

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.
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

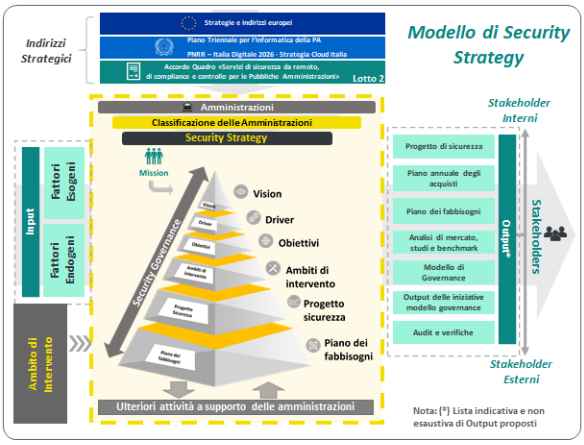
Il RTI si impegna a modificare o ampliare la composizione del team di progetto in funzione dell'operatività e dei deliverable richiesti, garantendo la disponibilità dei profili professionali e delle competenze previste.

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. Quest'ultimo, 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 (es. 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 Penetration Test (PT) rappresenta uno strumento fondamentale per identificare e gestire le vulnerabilità di sicurezza all'interno delle infrastrutture ICT delle Amministrazioni. Esso consente di simulare attacchi realistici per valutare la resilienza dei sistemi e delle applicazioni, garantendo al contempo la conformità alle normative vigenti e alle direttive di settore.

L'elaborazione del Progetto di Penetration Test (di seguito PT) si basa su modelli diversificati in relazione alla classificazione e complessità delle Amministrazioni (MappaPA). L'RTI prevede l'adozione di metodologie avanzate, sviluppate in conformità a standard riconosciuti a livello internazionale e leading practices nel campo della sicurezza ICT, tra cui OWASP, OSSTMM, PTES, NIST SP 800-115, ISO/IEC 27001-2, ISO/IEC 27034-1, e le Linee guida ENISA.

Attraverso tale approccio, l'Amministrazione sarà in grado di pianificare, implementare e monitorare efficacemente un programma di PT che risponda ai requisiti specifici del proprio contesto e alle esigenze di stakeholder interni ed esterni. Il PT mira a supportare la Missione dell'Amministrazione traducendola in una strategia operativa che includa misure preventive, rilevative e correttive per garantire la sicurezza delle informazioni e dei sistemi ICT.

Con riferimento agli ambiti di intervento del PT, per coprire l'intero ciclo di vita di un Penetration Test e assicurare un'analisi completa delle vulnerabilità, il RTI propone di considerare, a titolo indicativo e non esaustivo, i seguenti ambiti di intervento:

- Planning: Identificazione dell'ambito di test, definizione degli obiettivi e delle metodologie operative, assegnazione delle risorse e approvazione del piano di test.
- Pre-Engagement: Analisi preliminare del contesto, accordi di riservatezza (NDA), specifiche contrattuali, e chiarimenti sugli aspetti legali e sulla gestione delle responsabilità.
- Execution (Testing):
    - External Testing: Simulazione di attacchi provenienti dall'esterno per valutare l'esposizione pubblica.
    - Internal Testing: Test condotti come un attaccante interno, simulando scenari di minacce interne.
    - Application Security Testing: Analisi di sicurezza su applicazioni web e mobile, inclusi test basati sulle linee guida OWASP.
    - Network Penetration Testing: Valutazione della sicurezza delle infrastrutture di rete.
    - Wireless Security Testing: Test di sicurezza su reti wireless aziendali.
- Vulnerability Analysis: Identificazione e classificazione delle vulnerabilità riscontrate, valutazione del loro impatto e delle possibili vie di sfruttamento.
- Reporting:
    - Findings Report: Dettagli tecnici delle vulnerabilità con evidenze e livelli di criticità.
    - Executive Summary: Panoramica dei risultati per la dirigenza, con raccomandazioni strategiche.
- Post-Test Remediation:
    - Supporto nella definizione delle misure correttive e verifica della loro implementazione.
    - Re-Testing: Verifica delle correzioni effettuate.
- Compliance Assurance: Garanzia che i test soddisfino i requisiti di conformità normativa (es. GDPR, normative locali specifiche).