Identificativo: Piano Operativo V1

Data: 03/07/2023

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

LOTTO 2 – SERVIZI DI COMPLIANCE E CONTROLLO

PUBBLICHE AMMINISTRAZIONI LOCALI

Piano Operativo

Azienda Ospedaliera di Rilievo Nazionale e di Alta Specialità San Giuseppe Moscati

Costituito

Raggruppamento Temporaneo di Imprese

composto da:

Deloitte Risk Advisory S.r.l.

EY Advisory S.p.A.

Teleco S.r.l.

Deloitte. EY teleco

1 INTRODUZIONE

1.1 Ambito

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

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

Il presente documento costituisce il "Piano 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

Negli ultimi mesi gli attacchi informatici ad aziende sanitarie si sono moltiplicati, mettendo in serio pericolo i dati (e la salute) dei pazienti. Il settore sanitario, infatti, è molto appetibile per i cybercriminali, perché considerato uno dei più vulnerabili al pagamento dei riscatti (ransomware), per evitare la diffusione dei dati e proteggere le infrastrutture critiche. Negli ultimi anni, diverse strutture sanitarie sono state colpite da attacchi informatici che hanno causato la perdita di dati sensibili e il blocco dei sistemi informatici, impedendo ai medici di accedere ai dati dei pazienti e di erogare i servizi sanitari previsti.

In particolare, nelle strutture tecnologicamente più avanzate un crescente numero di apparecchiature elettromedicali e diagnostiche vengono interconnesse alle reti, accrescendo la possibilità di subire attacchi informatici. Questo è evidenziato dai molti episodi di ospedali colpiti da ransomware riportati dai media.

Le aziende ospedaliere devono fare i conti non solo con i rischi esterni, ma anche con quelli interni derivanti da personale non sufficientemente sensibilizzato ed una cultura aziendale non matura rispetto agli scenari di rischio emergenti.

Per questo motivo **A.O.R.N. San Giuseppe Moscati** ha deciso di ricevere un supporto qualificato per mantenere ed irrobustire la propria IT Security Posture, strutturando il proprio Sistema di Gestione della Sicurezza delle Informazioni (SGSI o ISMS in inglese) in conformità allo standard ISO/IEC 27001, intraprendendo il percorso verso la Certificazione formale del Sistema e gestendo un programma di test periodici sulla sicurezza applicativa dei propri sistemi simulandone la compromissione da parte di un attaccante esterno, identificando le vulnerabilità e sanandole in ottica di aumento dei livelli di sicurezza.

In tal senso è fondamentale attuare un continuo e programmato miglioramento della postura di sicurezza, con la formalizzazione dei processi virtuosi esistenti e nella cornice – più organizzata – di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI).

L'obiettivo è quello di rafforzare il governo e la maturità Cyber dell'**A.O.R.N. San Giuseppe Moscati,** ossia garantire Riservatezza, Integrità e Disponibilità del patrimonio informativo, con particolare

riferimento ai dati personali, nel contesto della digitalizzazione dei servizi dell'intero ecosistema. La progettualità include le seguenti attività:

- Assessment iniziale finalizzato una valutazione dettagliata delle attuali misure di sicurezza e dei rischi specifici insistenti sull'Azienda Ospedaliera, al fine di individuare eventuali aree di miglioramento;

Attività ciclica di processi continui nel tempo

- **Implementazione tecnica:** attraverso il supporto specialistico costante nelle azioni di rimedio e adozione degli strumenti tecnici necessari per affrontare le vulnerabilità individuate nelle attività di assessment, secondo il Programma di miglioramento continuo.
- **Formalizzazione, monitoraggio ed evoluzione dei processi organizzativi:** attraverso l'identificazione delle pratiche e processi virtuosi esistenti nell'ambito del U.O.C. Sistemi Informativi, formalizzazione degli stessi, per ottenere la maturità organizzativa necessaria ai fini della certificazione ISO27001:2022. Questo standard internazionale, ben noto e riconosciuto, fornisce un insieme di regole chiare e strutturate per organizzare le attività di sicurezza ed agevolare la conformità agli obblighi di legge in materia di privacy e protezione dei dati personali (GDPR).
- **Valutazione tecnica periodica e monitoraggio continuo:** per supportare il monitoraggio costante dello stato delle misure di sicurezza ed individuare eventuali nuove vulnerabilità ottenendo i dati necessari per le iniziative di rimedio. Questo processo consiste in due attività cicliche:
  - **Vulnerability Assessment (VA):** valuta periodicamente le vulnerabilità esistenti in ragione delle minacce;
  - **Penetration Test (PT):** verifica l'effettiva efficacia delle misure di sicurezza adottate a contrasto delle minacce.

Nell'ambito del contratto quadro per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni, l'A.O.R.N. San Giuseppe Moscati ha richiesto, ai fini dello sviluppo del **Progetto di Sicurezza,** l'esecuzione dei servizi afferenti al **Lotto 2- Servizi di Compliance e controllo:**

- **L2.S16 Servizio di Security Strategy;**
- **L2.S17 Servizio di Vulnerability Assessment;**
- **L2.S21 Supporto all'Analisi e alla Gestione degli Incidenti;**
- **L2.S22 Servizio di Penetration Testing;**
- **L2.S23 Compliance Normativa.**

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
…	
Inserire altri acronimi specifici dei servizi richiesti	

2 Anagrafica dell'amministrazione

DATI ANAGRAFICI DELL'AMMINISTRAZIONE	
Ragione sociale Amministrazione	Azienda Ospedaliera di Rilievo Nazionale
Indirizzo	C.da Amoretta
CAP	83100
Comune	Avellino
Provincia	AV
Regione	Campania
Codice Fiscale	01948180649
Indirizzo mail	info@aornmoscati.it
PEC	protocollo.generale@pec.aornmoscati.it
Codice PA	ao_sgma
Comparto di Appartenenza (PAL/PAC)	PAL

DATI ANAGRAFICI REFERENTE DELL'AMMINISTRAZIONE	
Nome	Giuseppe
Cognome	Versace
Telefono	
Indirizzo mail	giuseppe.versace@aornmoscati.it
PEC	

3 CATEGORIZZAZIONE DELL'INTERVENTO

3.1 Categorizzazione di I livello

Contrassegnare con la X l'ambito o gli ambiti 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

L'ambito funzionale del **Progetto di Sicurezza** dell'A.O.R.N. San Giuseppe Moscati è prevalentemente finalizzato a rafforzare il governo e la maturità di Sicurezza dell'Azienda Ospedaliera, ossia garantire Riservatezza, Integrità e Disponibilità del patrimonio informativo nel contesto della digitalizzazione dei servizi erogati.

Nel corso degli ultimi anni U.O.C. Sistemi Informativi ha intrapreso e finalizzato importanti interventi volti al miglioramento della stabilità dei sistemi informativi mediante il consolidamento dell'infrastruttura fisica e logica (a titolo esemplificativo e non esaustivo: Data center, server, rete, programmi di realizzazione di ambienti virtuali, backup e continuità operativa, antivirus e piattaforme per la sicurezza preventiva). In tale contesto ed al fine di continuare nel processo di consolidamento dei Sistemi Informativi, la Direzione del Dipartimento suggerisce un approccio progettuale che implica l'adozione di una strategia focalizzata sull'analisi e sullo sviluppo costante della postura di sicurezza, adatta al contesto attuale.

L'obiettivo è assicurare un aggiornamento continuo in relazione all'evolversi del panorama dei rischi ed in aggiunta e coerentemente a quanto già implementato nel corso degli ultimi anni mediante la pianificazione e l'esecuzione di specifiche attività caratterizzate da una valenza temporale una tantum, altre caratterizzate da una ciclicità di processi continui nel tempo, secondo la metodologia Plan-Do-Check-Act.

Tale strategia può portare numerosi benefici all'azienda, fra cui principalmente:

- la realizzazione di un Programma di miglioramento, unitario e coerente, idoneo a prevenire e contrastare le minacce informatiche dirette ai pazienti e all'Azienda Ospedaliera;
- la conformità alle principali normative e standard di settore, quali le "Misure Minime di Sicurezza" indicate dall' Agenzia Italia Digitale (AgID), le indicazioni dell'Agenzia Nazionale per la cybersicurezza Nazionale (ACN) la normativa nazionale in materia di cybersecurity, Regolamento Europeo Protezione dei Dati (GDPR) e lo standard ISO 27001:2022, che rappresenta una cornice unitaria e agevolatrice per la gestione della sicurezza informatica;

permettendo, così, di affrontare le crescenti sfide date dall'evoluzione tecnologica, attraverso il monitoraggio, la prevenzione e la risposta continua.

Il programma altresì consentirà all'Azienda, ed in particolare al perimetro di azione del U.O.C. Sistemi Informativi, l'ottenimento della certificazione ISO27001:2022.

4.2 Servizi richiesti

ID	NOME SERVIZIO	VOCE DI COSTO	QUANTITA'	VALORE ECONOMICO
L2.S16	Security Strategy	L2.S16 - gg/p Team ottimale	1.798	**449.500,00 €**
L2.S17	Vulnerability assessment	L2.S17 - gg/p Team ottimale	873	**144.000,00 €**
L2.S21	Supporto all'analisi e gestione degli incidenti	L2.S21 - gg/p Team ottimale	147	**25.000,00 €**
L2.S22	Penetration testing	L2.S22 - gg/p Team ottimale	461	**76.000,00 €**
L2.S23	Compliance normativa	L2.S23 - gg/p Team ottimale	70	**12.000,00 €**
			TOTALE	**706.500,00 €**

4.3 Dettaglio dei servizi richiesti

4.3.1 L2.S16 - Security Strategy

4.3.1.1 Descrizione e caratteristiche del servizio

Macro-Attività	Attività	Deliverable
Percorso ISO27001 – Primo anno – Attività propedeutiche e preparatorie	Definizione degli aspetti operativi e metodologici per la realizzazione del lavoro. In particolare: ➢ Obiettivi e il campo di applicazione del SGSI (U.O.C. Sistemi Informativi) ➢ Perimetro di dettaglio in termini di servizi, asset e dipartimenti coinvolti ➢ Elenco preliminare della documentazione che verrà visionata e sviluppata (es. politica per la sicurezza delle informazioni, organigramma, processi e procedure relative all'analisi del rischio) ➢ Modalità di condivisione dei risultati delle diverse fasi di lavoro.	Piano di lavoro di dettaglio Presentazione per il primo workshop informativo
Percorso ISO27001 – Primo anno – Assessment e Pianificazione	Realizzazione di interviste e verifiche orientate a comprendere lo stato dell'arte e gli interventi documentali ed operativi da realizzare all'interno dell'U.O.C.	Output interviste referenti Assessment Report e roadmap di pianificazione degli

		interventi
Percorso ISO27001 – Primo anno – Disegno del SGSI	Progettazione del SGSI e delle sue componenti, in termini di: ➢ Redazione del modello di servizi e processi adottato, con riferimento al perimetro di certificazione ➢ Disegno della struttura organizzativa e operativa del SGSI (es. ruoli e responsabilità, asset coinvolti); ➢ Redazione del corpo documentale di Policy allineate ai domini ISO27001 e del «ISO27001 specific kit»	ISO 27001 Policies ISO 27001 Specific Kit Modello servizi e processi
Percorso ISO27001 – Primo anno – Analisi dei rischi di sicurezza	Esecuzione di Security Risk Assessment sulla base della metodologia definita	Risk Assesment
Percorso ISO27001 – Primo anno – Formazione	Erogazione di sessioni di formazione in aula fisica e/o virtuale: ➢ N.1 Corso rivolto alla Direzione con finalità formative sugli elementi strategici dell'ISMS (es. Direzione Amministrativa). ➢ N.1 Corso per gli addetti operativi del SGSI (come il personale IT) sui principali temi di IT Security al fine di approfondire conoscenza sulle minacce e le tecniche di risposta agli attacchi. ➢ N.1 Corso rivolto a tutto il personale aziendale (o sotto-insieme maggiormente coinvolto nel Sistema). Il corso verterà sugli elementi fondamentali del Sistema, sulle procedure implementate, ponendo particolare attenzione agli aspetti più operativi.	Materiale didattico e Test di apprendimento per ciascuna delle sessioni di formazione Erogazione di n° 3 sessioni di formazione
Percorso ISO27001 – Primo anno – Audit del Sistema di Gestione	In questa fase verrà pianificato e svolto un audit interno del Sistema di gestione con l'obiettivo di: ➢ Verificare il grado di funzionamento del Sistema di Gestione e di applicazione delle relative procedure. ➢ Individuare eventuali aree critiche di funzionamento del sistema. ➢ Riportare alla Direzione i risultati.	Piano di Audit interno Verbale di Audit Interno
Percorso ISO27001 – Primo anno – Riesame del Sistema	L'attività di riesame prevede un supporto nelle seguenti azioni: ➢ Calcolare gli indicatori precedentemente definiti allo scopo di misurare l'efficacia del Sistema di Gestione (indicatori sia tecnici come, ad esempio, numero incidenti/breach e rilevazioni emerse dall'analisi dei rischi/audit); ➢ Esaminare i dati e le informazioni raccolte all'interno del SGSI (es. esiti del Risk	Relazione di Input per la Management Review Management Review

	Assessment e degli Audit, feedback Formazione); ➢ Revisionare il Sistema ai fini del suo miglioramento.	
Percorso ISO27001 – Primo anno – Assistenza alla Certificazione	Questa attività è orientata ad assistere il personale, durante le giornate di visite ispettive esterne condotte dall'Ente di Certificazione* e saranno finalizzate al riscontro dell'effettiva aderenza del SGSI alla Norma ISO 27001: ➢ Sia per quanto riguarda la documentazione predisposta ➢ Sia per le attività effettivamente messe in atto. Verrà inoltre fornita assistenza nell'interlocuzione con l'Ente di certificazione e supporto nella gestione delle richieste dell'Ente e delle eventuali osservazioni, che verranno formalizzate in un "Piano di adeguamento", nel quale saranno suggeriti tempi, risorse e responsabilità per la loro risoluzione.	Sintesi dei risultati riscontrati durante le verifiche Piano per la chiusura di eventuali osservazioni rilasciate dal certificatore
Percorso ISO27001 – Primo anno – Supporto Specialistico per la valutazione dei controlli tecnologici	Durante il percorso di certificazione emergerà la necessità di svolgere attività di supporto al fine di indirizzare azioni tecniche. A titolo esemplificativo e non esaustivo: ➢ Controlli applicativi. Supporto all'identificazione e alle configurazioni sui sistemi di autenticazione applicativa. Interazioni con i sistemi di certificazione a chiave pubblica e privata. Supporto all'identificazione delle vulnerabilità e alle mitigazioni da applicare su sistemi applicativi ➢ Controlli infrastrutturali.	Report periodici di stato avanzamento
Percorso ISO27001 – Secondo anno – Supporto Specialistico al mantenimento della certificazione	➢ Revisione del SGSI; ➢ Aggiornamento del Risk Assessment e rielaborazione dei risultati; ➢ Sessione formativa di aggiornamento e refresh; ➢ Esecuzione audit su 1 ambito/processo e 1 fornitore critico; ➢ Riesame del sistema; ➢ supporto al team durante la visita del certificatore; ➢ controlli applicativi ed infrastrutturali.	Come per attività previste per il primo anno, esclusi output relativi ad "attività propedeutiche e preparatorie" e "Assesment e pianificazione"
Attività di supporto System Hardening	Supporto alla revisione delle configurazioni dei sistemi a seguito degli esiti delle attività di VA-PT	Eventuale revisione delle configurazioni dei sistemi

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 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, per il primo anno e per l'anno successivo, 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 prevede l'avvio del servizio entro Luglio 2023 per una durata di 24 mesi.

4.3.2 L2.S17 - Vulnerability assessment

4.3.2.1 Descrizione e caratteristiche del servizio

Macro-Attività	Attività	Deliverable
Vulnerability Assessment	Cyber Testing volto all'identificazione delle capacità dei sistemi e degli strumenti di sicurezza mediante	Executive Summary
	➢ Attività Vulnerability Assessment su un sottoinsieme dei sistemi IT rilevante dell'Ente	Technical Report
	➢ Definizione del piano di azione e supporto all'identificazione delle modalità di implementazione	Remediation Plan
	➢ Re-check delle vulnerabilità a seguito del remediation plan	

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 consuntivazione avverrà sulla base dello stato dell'avanzamento lavori mensile determinato coerentemente con il piano di lavoro definito.
Il team di lavoro per la realizzazione delle attività sopraccitate prevede il coinvolgimento delle seguenti figure professionali:

- Security Principal

- Senior Penetration tester
- Junior Penetration tester

Le attività, per il primo anno e per l'anno successivi, saranno erogate presso le sedi dell'Amministrazione Contraente e da remoto (es: presso le sedi del RTI).

4.3.2.3 Attivazione e durata

Si prevede l'avvio del servizio entro Luglio 2023 per una durata di 24 mesi.

4.3.3 L2.S21 - Supporto all'analisi e gestione degli incidenti

4.3.3.1 Descrizione e caratteristiche del servizio

Macro-Attività	Attività	Deliverable
Miglioramento del processo di Incident Management	Analisi e miglioramento del processo di incident management (rilevazione, risposta agli incidenti, playbook e processi di gestione della crisi)	Processo di Incident Management

4.3.3.2 Modalità di erogazione e consuntivazione

Coerentemente a quanto previsto nel "CAPITOLATO TECNICO SPECIALE SERVIZI DI COMPLIANCE E CONTROLLO" si precisa che la modalità di remunerazione di tali servizi è "progettuale (a corpo)" e che la metrica di misurazione è "*giorni/persona*".
Saranno definiti di concerto con l'Amministrazione dei task e dei deliverable, dimensionati e valorizzati economicamente. La consuntivazione avverrà sulla base dello stato dell'avanzamento lavori mensile determinato coerentemente con il piano di lavoro definito.
Il team di lavoro per la realizzazione delle attività sopraccitate prevede il coinvolgimento delle seguenti figure professionali:

- Security Principal
- Senior Security Analyst
- Junior Security Analyst
- Forensic Expert

Le attività, per il primo anno e per l'anno successivo, saranno erogate presso le sedi dell'Amministrazione Contraente e da remoto (es: presso le sedi del RTI).

4.3.3.3 Attivazione e durata

Si prevede l'avvio del servizio entro Luglio 2023 per una durata di 24 mesi.

4.3.4 L2.S22 - Penetration testing

4.3.4.1 Descrizione e caratteristiche del servizio

Macro-Attività	Attività	Deliverable
Penetration Testing	Cyber Testing volto all'identificazione delle capacità dei sistemi e degli strumenti di sicurezza mediante ➢ Attività Penetration Test su un sottoinsieme dei sistemi IT rilevante dell'Ente	Executive Summary Technical Report

	➢ Definizione del piano di azione e supporto all'identificazione delle modalità di implementazione ➢ Re-check delle vulnerabilità a seguito del remediation plan	Remediation Plan

4.3.4.2 Modalità di erogazione e consuntivazione

Coerentemente a quanto previsto nel "CAPITOLATO TECNICO SPECIALE SERVIZI DI COMPLIANCE E CONTROLLO" si precisa che la modalità di remunerazione di tali servizi è "progettuale (a corpo)" e che la metrica di misurazione è "*giorni/persona*".
Saranno definiti di concerto con l'Amministrazione dei task e dei deliverable, dimensionati e valorizzati economicamente. La consuntivazione avverrà sulla base dello stato dell'avanzamento lavori mensile determinato coerentemente con il piano di lavoro definito.
Il team di lavoro per la realizzazione delle attività sopraccitate prevede il coinvolgimento delle seguenti figure professionali:

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

Le attività, per il primo anno e per il secondo anno, saranno erogate presso le sedi dell'Amministrazione Contraente e da remoto (es: presso le sedi del RTI).

4.3.4.3 Attivazione e durata

Si prevede l'avvio del servizio entro Luglio 2023 per una durata di 24 mesi.

4.3.5 L2.S23 - Compliance normativa

4.3.5.1 Descrizione e caratteristiche del servizio

Macro-Attività	Attività	Deliverable
Governo della Conformità Privacy	Supporto operative nelle attività di consolidamento del livello di Compliance Normativa in ambito Privacy con riferimento al perimetro del SGSI (U.O.C. Sistemi Informativi).	Set documentale in ambito Privacy

4.3.5.2 Modalità di erogazione e consuntivazione

Coerentemente a quanto previsto nel "CAPITOLATO TECNICO SPECIALE SERVIZI DI COMPLIANCE E CONTROLLO" si precisa che la modalità di remunerazione di tali servizi è "progettuale (a corpo)" e che la metrica di misurazione è "*giorni/persona*".
Saranno definiti di concerto con l'Amministrazione dei task e dei deliverable, dimensionati e valorizzati economicamente. La consuntivazione avverrà sulla base dello stato dell'avanzamento lavori mensile determinato coerentemente con il piano di lavoro definito.
Il team di lavoro per la realizzazione delle attività sopraccitate prevede il coinvolgimento delle seguenti figure professionali:

- Security Principal

- Senior Information Security Consultant
- Junior Information Security Consultant
- Senior Security Auditor
- Data Protection Specialist

Le attività, per il primo anno e per il secondo anno, saranno erogate presso le sedi dell'Amministrazione Contraente e da remoto (es: presso le sedi del RTI).

4.3.5.3 Attivazione e durata

Si prevede l'avvio del servizio entro Luglio 2023 per una durata di 24 mesi.

5 Organizzazione e modalità di erogazione del contratto esecutivo

5.1 Organizzazione e figure di riferimento del fornitore

Si riportano di seguito il personale incaricato dall'Amministrazione con i relativi ruoli/responsabilità.

RUOLO	NOMINATIVI
U.O.C. Sistemi Informativi	Direttore U.O.C.

5.2 Attività in carico alle aziende del RTI

SERVIZIO	Deloitte Risk Advisory (%)	EY Advisory (%)	Teleco (%)
L2.S16	0 %	100 %	0 %
L2.S17	0 %	100 %	0 %
L2.S21	0 %	100 %	0 %
L2.S22	0 %	100 %	0 %
L2.S23	0 %	100 %	0 %
TOTALE	0 %	100 %	0 %

5.3 Modalità di ricorso al subappalto da parte del fornitore

SERVIZIO	AZIENDA RTI	QUOTA SUBAPPALTABILE	SUBAPPALTATORE
L2.S16, L2.S17, L2.S21, L2.S22, L2.S23	**DLT R.A.- EY-TELECO**	**50%**	**DA DEFINIRE**

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.

5.4 Organizzazione e figure di riferimento del fornitore

RUOLO	NOMINATIVI
RUAC CE	Rodolfo Mecozzi
Referente Tecnico CE (RT)	Rodolfo Mecozzi
Responsabile Attività L2.S16	Rodolfo Mecozzi
Responsabile Attività L2.S17	Rodolfo Mecozzi
Responsabile Attività L2.S21	Rodolfo Mecozzi
Responsabile Attività L2.S22	Rodolfo Mecozzi

Responsabile Attività L2.S23	Rodolfo Mecozzi

5.5 Modalità di esecuzione dei servizi

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

6 Piano di lavoro

6.1 Piano di Presa in carico

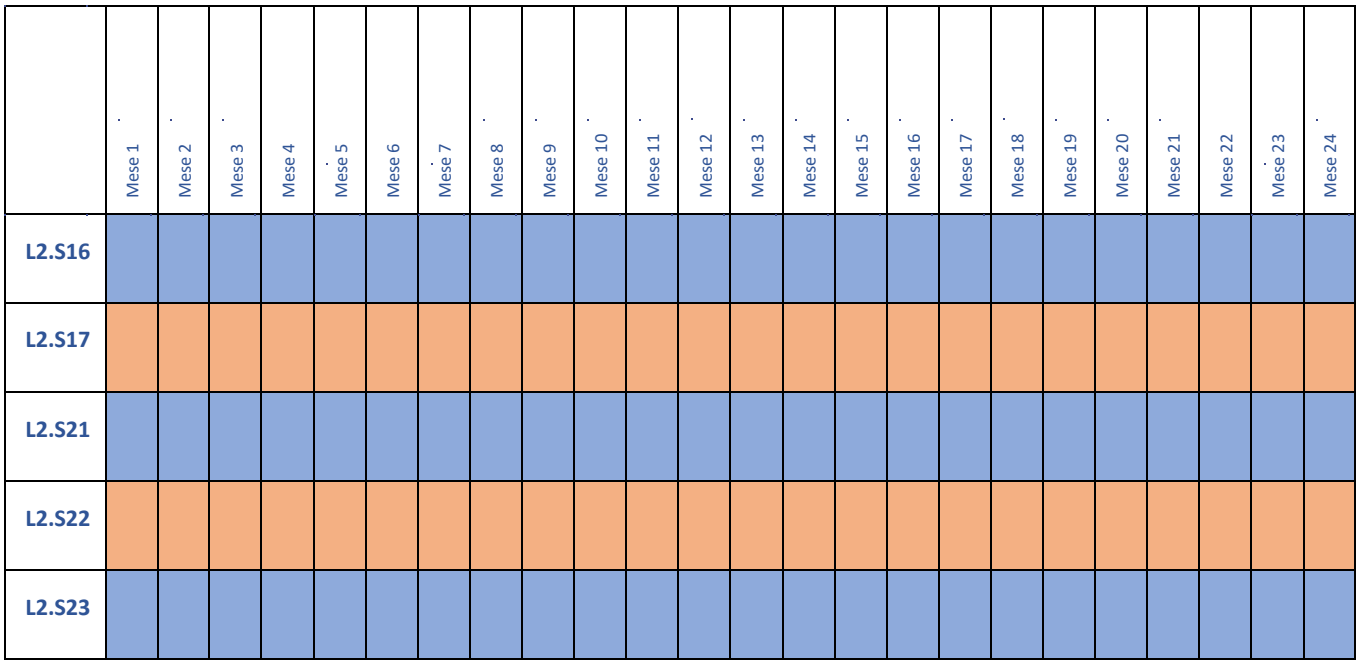
Il piano di presa in carico si basa sul coinvolgimento del personale che verrà poi impegnato a regime nella fornitura, sia a livello di governo che di erogazione dei servizi e trasparenza sull'andamento del processo di subentro nei confronti di tutti gli attori interessati attraverso una governance operativa e focalizzata.

FASE	ATTIVITÀ	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 e del fornitore uscente, 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					

6.2 Cronoprogramma

La durata ipotizzata per la fornitura è di 24 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.



6.3 Data di attivazione e durata del servizio

Il contratto esecutivo avrà i suoi effetti dalla data di stipula, avrà una durata di **24 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.

Vulnerability Assessment (L2.S17)

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 Penetration tester	Definito anche ethical hacker, tenta di penetrare in un sistema informatico allo scopo di verificarne la relativa sicurezza rispettando opportune regole concordate in fase di ingaggio. Responsabile del coordinamento delle figure più Junior.
Junior Penetration tester	Definito anche ethical hacker, tenta di penetrare in un sistema informatico allo scopo di verificarne la relativa sicurezza rispettando opportune regole concordate in fase di ingaggio

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.

Supporto all'analisi e gestione degli incidenti (L2.S21)

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 Security Analyst	Gestisce l'esame periodico della sicurezza di sistemi, reti e applicazioni evidenziando le vulnerabilità tecniche nonché gli eventuali scostamenti rilevati rispetto e regole interne, normative esterne e best practices internazionali in materia Responsabile del coordinamento delle figure più Junior.
Junior Security Analyst	Gestisce l'esame periodico della sicurezza di sistemi, reti e applicazioni evidenziando le vulnerabilità tecniche nonché gli eventuali scostamenti rilevati rispetto e regole interne, normative esterne e best practices internazionali in materia.
Forensic Expert	E' chiamato a gestire la raccolta di evidenze e l'analisi delle stesse in concomitanza di un incidente relativo alla sicurezza delle informazioni documentando il tutto in modo che sia correttamente presentabile in sede processuale.

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 Testing (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 Penetration tester	Definito anche ethical hacker, tenta di penetrare in un sistema informatico allo scopo di verificarne la relativa sicurezza rispettando opportune regole concordate in fase di ingaggio. Responsabile del coordinamento delle figure più Junior.
Junior Penetration tester	Definito anche ethical hacker, tenta di penetrare in un sistema informatico allo scopo di verificarne la relativa sicurezza rispettando opportune regole concordate in fase di ingaggio
Forensic Expert	E' chiamato a gestire la raccolta di evidenze e l'analisi delle stesse in concomitanza di un incidente relativo alla sicurezza delle informazioni documentando il tutto in modo che sia correttamente presentabile in sede processuale.

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.

Compliance normativa (L2.S23)

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.
Junior Information Security Consultant	Contribuisce nell'attuazione della strategia definita all'interno del suo ambito di responsabilità (sia questo un progetto, un processo, una location) partecipando al ruolo di 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.
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

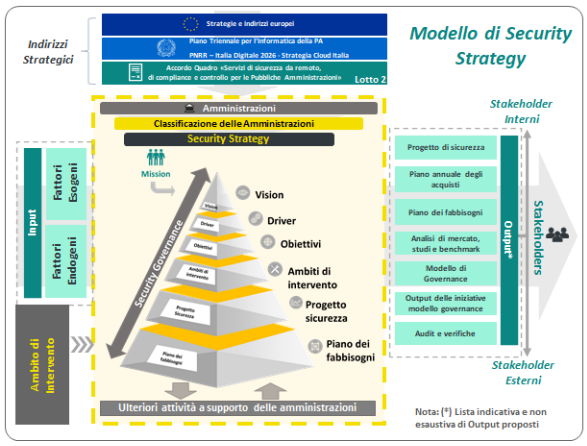
Il RTI si impegna a modificare o ampliare la composizione del team di progetto in funzione dell'operatività e dei deliverable richiesti, garantendo la disponibilità dei profili professionali e delle competenze previste.

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:



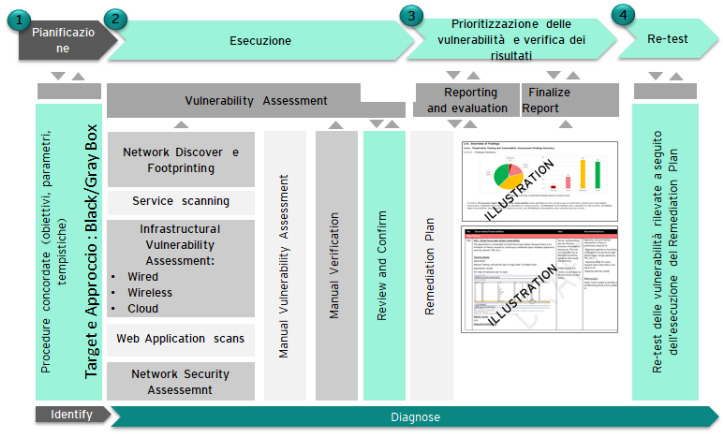
- Identify: strategia e pianificazione, Governance Asset e Processi, gestione del rischio cyber, security assurance (VA, PT, Testing del Codice), sicurezza terze parti e contratti di servizio, Compliance normativa;
- Protect (Management): Information & Data Security, Identity & Access Management, Security 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.

Vulnerability Assessment (L2.S17)

Il servizio di Vulnerability Assessment prevede l'identificazione in maniera proattiva, mediante una verifica dinamica della sicurezza, delle vulnerabilità presenti su dispositivi di rete, software e applicazioni delle Amministrazioni e la mitigazione dei rischi cyber connessi. Il RTI eroga le attività in ambito al presente servizio facendo affidamento sugli elementi distintivi sotto riportati.
1. Standardizzazione del reporting e dei piani di prioritizzazione/remediation attraverso l'utilizzo di una piattaforma centralizzata (denominata Bug Blast) ed indipendente dai motori di scansione (vulnerability scanner), garantendo ripetibilità ed uniformità dei risultati;
2. Metodologia per la definizione dei "remediation plan" con approccio risk-based e reportistica in grado di rappresentare le vulnerabilità identificate sia ad interlocutori executive che tecnici, fornendo pratici strumenti operativi per agevolare la risoluzione delle stesse;
3. Centri di eccellenza nazionali ed internazionali in ambito Cybersecurity (Roma, Milano, Bari, ed oltre 10 in EU), con la presenza di laboratori specialistici e con professionalità verticali su attività di Offensive Security. Tali centri supportano i team nella raccolta di informazioni relative a nuove vulnerabilità (es. mediante tecniche di Cyber Threat Intelligence) e tecniche innovative per lo sfruttamento delle stesse;

4. Eterogeneità nella copertura degli ambienti target (IT/OT/IoT/Cloud) attraverso strumenti e tecniche idonee e specifiche a garantire il discovery per ciascuna tipologia di target;
5. Ampio supporto nel discovery di misconfiguration e vulnerability specifiche per gli ambienti di cloud computing (IaaS, PaaS, SaaS), anche in presenza di CSP differenti (AWS, Azure, Google, ecc.).

Le attività di Vulnerability Assessment (VA) forniranno evidenze di dettaglio sulle vulnerabilità riconducibili all'infrastruttura ICT e IoT/OT (, funzionali anche ad elaborare una baseline iniziale del livello di vulnerabilità e di esposizione del sistema informativo dell'Amministrazione. L'attività sarà svolta sia con strumenti automatici sia con strumenti definiti ad-hoc sulla base della tipologia del target oggetto di analisi. Il RTI, sulla base della propria esperienza e del contesto di riferimento in cui saranno svolte le analisi di sicurezza, proporrà gli strumenti di analisi più adatti per l'esecuzione dei VA. Le attività di VA eseguite sono basate sulle metodologie OSSTMM, OWASP, PTES, NIST 800-52/53 e ISA 62443, riconosciute globalmente come standard de-facto.



L'applicazione di tali metodologie garantirà risultati coerenti, ripetibili e misurabili. Nell'ambito delle attività di VA terremo in considerazione il sempre più diffuso utilizzo delle tecnologie Cloud da parte delle Amministrazione, in coerenza con quanto definito dalla Strategia Cloud Italia. A tal fine, su specifica richiesta dell'Amministrazione, il RTI è in grado di integrare all'interno dei servizi offerti anche l'esecuzione di attività di Assessment del livello di sicurezza dei servizi Cloud IaaS e SaaS, verificandone la compliance rispetto a standard, requisiti normativi e best practice di settore, e ricercando vulnerabilità celate negli errori di configurazione dei diversi ambienti cloud. Il RTI potrà eseguire le attività di VA in maniera periodica ove richiesto e ritenuto opportuno.
Per l'esecuzione dei servizi richiesti dall'Amministrazione, la metodologia prevede l'esecuzione di 4 fasi progettuali:

- Pianificazione delle attività,
- Esecuzione dei Vulnerability Assessment,
- Proritizzazione delle vulnerabilità e verifica dei risultati,
- Re-test delle vulnerabilità a seguito del remediation plan.

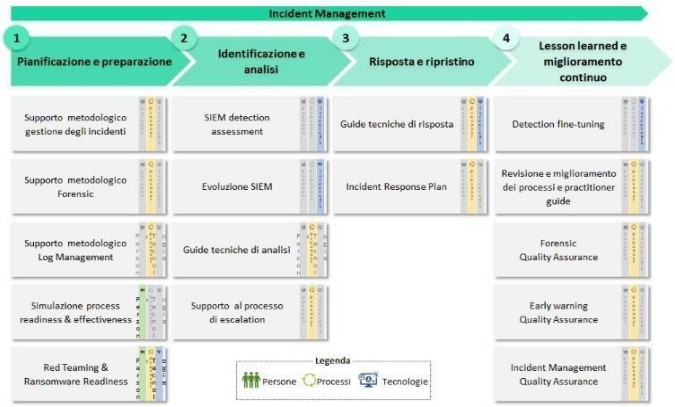
Il RTI propone l'adozione di una piattaforma specifica per l'esecuzione di attività di Vulnerability Assessment. La Piattaforma Bug Blast ha l'obiettivo di fornire report personalizzati e di tracciare le vulnerabilità dalla fase di discovery e per tutte le fasi di remediation. Le informazioni che afferiscono alle attività di VA richieste saranno disponibili nel portale tramite un sistema di autorizzazione granulare e le Amministrazioni potrà accedere a tali informazioni sulla base del periodo di retention che sarà concordato di volta in volta con le stesse e comunque, salvo diversa indicazione da parte dell'Amministrazione e nel rispetto delle normative vigenti, per un periodo garantito non inferiore a 1 mese dalla fine delle attività. Tale modalità di erogazione è consigliata dal RTI, che tuttavia è disponibile ad adattare la stessa sulla base di eventuali esigenze delle Amministrazioni, concordandole di volta in volta con le stesse. Approccio operativo. L'approccio operativo proposto dal RTI prevede l'esecuzione di tutte le attività tecniche previste dal CTS. I relativi risultati saranno analizzati e correlati dal Team operativo. Ove possibile, per le vulnerabilità rilevate sarà effettuata una verifica manuale al fine di identificare ed eliminare i falsi positivi; tale attività è svolta mediante processi innovativi di controllo, sviluppati nel corso delle esperienze in ambito Offensive Security e tramite il supporto dei Centri di eccellenza del RTI, che consentono di ridurre al minimo la presenza di errori.

Di seguito sono riportati i principali strumenti/soluzioni tecnologiche che saranno utilizzati per l'erogazione del servizio:

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

Supporto all'analisi e gestione degli incidenti (L2.S21)

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



1. Coinvolgimento di risorse con ampia e riconosciuta esperienza nella realizzazione di CERT e SOC in Italia e nel mondo per organizzazioni pubbliche e private di primaria importanza. Il RTI ha inoltre supportato 7 delle 11 organizzazioni italiane che hanno accreditato i loro CERT alla community internazionale FIRST
2. Coinvolgimento di risorse che hanno contribuito direttamente allo sviluppo delle pratiche di Incident Readiness come dimostrato dalla pubblicazione di numerosi studi nazionali e internazionali.
3. Disponibilità di una libreria proprietaria composta da oltre 350 Use Case di monitoraggio costantemente aggiornata sulla base delle esperienze acquisite presso i clienti del network a livello globale, evoluzioni tecnologiche, trasformazioni nelle tattiche, tecniche e procedure (TTP) utilizzate dagli attori di minaccia in diverse tipologie di ambienti (es. cloud SaaS, PaaS e IaaS, Mobile, IoT, ecc.)
4. Disponibilità di framework proprietari, sviluppati internamente dal RTI e aggiornati in maniera continuativa sulla base delle esperienze acquisite e di report specialistici di settore, per la valutazione del livello di maturità di CERT e SOC e l'identificazione delle tecnologie di sicurezza a supporto delle attività di gestione degli incidenti
5. Team di lavoro multidisciplinare altamente qualificato e certificato in ambito Forensic, Security Defense e Offense.

Il servizio di supporto all'analisi e gestione degli incidenti proposto affronta la tematica in modo olistico e multidisciplinare. Al fine di raggiungere tali obiettivi, il RTI supporta l'Amministrazione al fine di abilitare il corretto svolgimento di ciascuna delle fasi di gestione degli incidenti attraverso attività consulenziali da svolgersi in maniera preventiva come supporto all'intero processo (analisi e progettazione) e definire un processo strutturato di Forensic e verificarne l'efficacia (verifica).

A) Incident Management

Il RTI propone un approccio strutturato al supporto in ambito gestione incidenti, che prevede l'esecuzione di attività di natura consulenziale da svolgersi preventivamente per guidare il corretto svolgimento del servizio di Incident Management da parte dell'Amministrazione. Ciascuna delle attività proposte consentirà di abilitare lo svolgimento e incrementare l'efficacia di una diversa fase del processo di Incident Management, come di seguito riportato:

- A.1 Pianificazione e preparazione: una fase di preparazione correttamente eseguita e personalizzata sulla base del contesto permette di minimizzare gli impatti degli incidenti, facendo leva su un'adeguata infrastruttura tecnologica di sicurezza e personale specializzato.
- **A.2 Identificazione e analisi:** la fase di identificazione e analisi di un incidente ha l'obiettivo di monitorare in modo centralizzato gli eventi di sicurezza provenienti da fonti strutturate (es. SIEM) e non strutturate (es. e-mail da utenti) per rilevare minacce miranti agli asset e ai servizi della PA, analizzarli per comprendere se si tratti di un falso positivo che necessita di azioni correttive o di un incidente con potenziale impatto sul perimetro e classificare e prioritizzarne la gestione sulla base di criteri definiti.
- **A.3** Risposta e ripristino: tale fase prevede l'identificazione e l'implementazione delle azioni di contenimento a breve termine dell'incidente, con l'obiettivo di limitare le conseguenze dell'incidente e ripristinare la normale operatività in maniera tempestiva ed efficace.
- **A.4 Lesson** learned e miglioramento continuo: tale fase prevede, immediatamente a valle della gestione di un incidente, una valutazione ex-post della stessa per verificare che le attività siano state condotte in conformità con quanto previsto dal processo, e un'attività periodica volta a identificare eventuali punti di miglioramento nelle attività svolte attraverso l'elaborazione di reportistica, lo svolgimento di meeting ricorrenti per condividere eventuali gap e relative azioni di rimedio.

B) Forensic

Le attività di supporto all'Amministrazione nella gestione di incidenti di sicurezza prevedono un approccio sinergico, finalizzato a incrementare l'efficienza delle modalità di intervento e dei tempi di reazione da parte dell'Amministrazione, in particolare nell'analisi forense post-mortem degli incidenti.

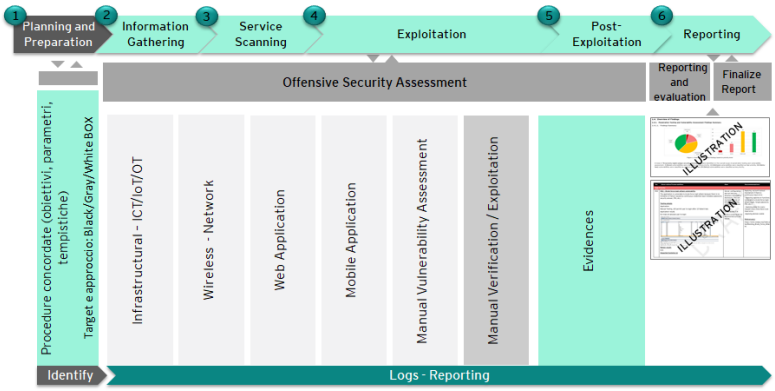
Le attività di supporto erogate nei confronti dell'Amministrazione prevedranno una costante verifica di quality assurance da parte di profili esperti, al fine di garantire un elevato livello qualitativo dell'esecuzione del processo di Forensic.

- Definizione di un template di catena di custodia per supportare i team di Forensic nel tracciamento delle attività eseguite sulle evidenze acquisite;
- Definizione di un processo di Forensic secondo best practice volto a definire ruoli, responsabilità, principi e attività operative che regolano il processo stesso;
- Governo (organizzazione, pianificazione, coordinamento, controllo) delle attività di verifica tecnica (quality assurance) del processo di Forensic.

Penetration Testing (L2.S22)

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

1. Eccellenza del team di Ethical Hacking dimostrata dalla pubblicazione regolare di Common Vulnerabilities and Exposures (CVE) elenco di vulnerabilità divulgate pubblicamente e Zero Day, condivise attraverso i metodi di "Responsible Disclosure";
2. Copertura completa dei principali vettori di attacco per ogni singola sessione e tipologia di target, acquisita mediante l'aggiornamento continuo di un archivio centralizzato contenente il Threat Modelling e relative Tactics, Techniques and Procedures (TTP), alimentato dal team di Pen Tester coinvolti a livello globale nell'erogazione di tali servizi;



3. Utilizzo estensivo di fonti Cyber Threat Intelligence (OSINT e CLOSINT) con copertura geografica mondiale, derivante dai servizi di sicurezza gestista (SOC) del RTI, che consentono al Pen Tester di ottenere un quadro più ampio dell'effettivo livello di esposizione dei target in analisi, come ad esempio compromissioni/vulnerabilità/tecniche pubblicate nel dark web o in community specifiche, potenzialmente accessibili anche agli attaccanti e sfruttabili per realizzare una reale compromissione,;
4. Molteplicità di laboratori a livello nazionale ed internazionale con personale, strumenti ed infrastrutture dedicate alle attività di offensive security, con possibilità di verificare costantemente i vettori e le tecniche di attacco in ambienti simulati e su dispositivi di test; tali laboratori sono impiegati anche per addestramento, formazione ed aggiornamento continuo dei Pen Tester.

Di seguito sono riportati i principali strumenti/soluzioni tecnologiche che saranno utilizzati per l'erogazione del servizio.

Ambito di utilizzo	Principali strumenti
PT Infrastrutturale	● **Open Source**: nmap, netdiscovery, dnsrecon, dig, metasploit, netcat, masscan,scapy,hping, CrackMapExec, Air-Ng tools, Wifite, Airgeddon, Wireshark; ● **Di Mercato:** Acrylic WIFI **,** Hak5 Wifi (HW e SW), Nessus
PT Applicativo	● **Open Source**: Objection, Frida ,Apktool, Dex2jar, Hopper, Drozer, MobSF, Clang Static Analyzer, Andrubis, Flawfinder, ApkAnalyser, Androwarn, Ghidra, Radare; ● **Di Mercato:** Nessus, Burp Proxy Professional
PT Device IOT	● **Open Source**: Burp Proxy Professional, Blue Scanner, Blue Sniff, BlueBugger, BTBrowser, BTCrawler, BlueSnarfing, ZigDiggity; ● **Di Mercato:** HackRF, Proxmark
Red Team	● **Open Source**: Social Engineering Toolkit (SET) , Gophish , Invoke-Obfuscation, Veil Framework, Empire Project, DNSExfiltrator, Cloakify Factory; ● **Di Mercato:** Cobalt Strike, Metasploit Pro

Compliance normativa (L2.S23)

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

- Multidisciplinarietà delle competenze (IT, legali, operative e organizzative) integrate in team strutturati.

- Utilizzo del GDPR Compliance Framework (GDPR CF), che include la metodologia per lo svolgimento delle attività, modelli, processi, questionari, baseline di requisiti, strumenti automatizzati, in grado efficientare le attività progettuali
- Costante aggiornamento normativo realizzato attraverso l'Osservatorio Privacy del RTI
- DRA ed EYA si possono avvalere della collaborazione dei propri Studi Legali Associati.

Il Sistema di gestione della Privacy ha necessità di essere disegnato, analizzato, implementato, monitorato e continuamente migliorato in un'ottica anche di lungo periodo, al fine di trasformare la privacy in un fattore abilitante per il trattamento dei dati da parte dell'Amministrazione e garantire agli interessati la protezione dei dati personali. A tale scopo, il RTI utilizzerà, per guidare lo svolgimento delle attività, il GDPR Compliance Framework (GDPR CF). Tale strumento propone una metodologia per la definizione e mantenimento del sistema privacy ed è caratterizzato da un ciclo di 4 fasi: a) Analisi; b) Implementazione; c) Verifica; d) Continuous Improvement. Quest'ultima fase è abilitata dal Privacy Maturity Model (PMM), ovvero uno strumento in grado di intercettare nel continuo, i punti di forza e di miglioramento del Sistema di gestione della privacy esprimendo lo stato di maturità e identificando in modo dinamico le aree di intervento. L'utilizzo del GDPR CF, oltre a mettere a disposizione un set esaustivo di strumenti automatici, potrà, essere supportato da un prodotto software integrato che consente di gestire il Sistema Privacy in modalità condivisa e collaborativa tra tutti i soggetti interessati (es. DPO, Privacy Officer, IT, Sicurezza, Risorse Umane, Acquisti).
Analisi: la fase di analisi prevede lo svolgimento di un assessment per verificare lo stato di conformità alla normativa applicabile da parte delle Amministrazioni al fine di comprendere le aree maggiormente a rischio e identificare gli eventuali interventi di rimedio necessari per garantire conformità e allo stesso tempo automatizzare i processi privacy.
Implementazione. tale fase consentirà di indirizzare le azioni di rimedio emerse a seguito dell'Assessment ed incluse nel Piano degli interventi o già previste dai piani di conformità dell'Amministrazione. Allo scopo di massimizzare l'efficacia degli interventi e la logica del riuso, le attività di implementazione sono eseguite secondo un modello operativo che prevede la messa a disposizione di template consolidati per le componenti del framework documentale (es. politiche, procedure, metodologie, nomine a responsabile, informative, data processing agreement, materiale formativo) che saranno condivisi con l'Amministrazione e personalizzati sulla base delle specifiche necessità
Verifica: tale fase consente di misurare l'effettiva implementazione dei requisiti normativi a cui è soggetta l'Amministrazione, valutare il rischio derivante dai gap ed il livello di maturità raggiunto, proponendo eventuali punti di miglioramento, attraverso piani di azione costantemente monitorati.
Continuous Improvement: al fine di trasformare la privacy da adempimento di legge ad abilitatore "mandatorio" e cogliere tempestivamente i rischi normativi/sanzionatori/IT, si prevede l'adozione del PMM (o in alternativa il Data Protection Maturity Self-Assessment Model rilasciato dal CNIL).