ALLEGATO A – OFFERTA TECNICA DEL FORNITORE

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

Relazione Tecnica

INDICE

1 PREMESSA

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

2 PRESENTAZIONE E DESCRIZIONE OFFERENTE

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

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

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

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

- **Deloitte Risk Advisory S.r.l.**: **Lorenzo Fersurella**, [redacted] domiciliato per la carica presso la sede societaria in Milano, Via Tortona n. 25 – CAP 20144, nella sua qualità di Procuratore
- **EY Advisory S.p.A.**: **Dario Bergamo**, n[redacted] domiciliato per la carica presso la sede societaria in Milano, Via Meravigli n. 14 – CAP 20123, nella sua qualità di Procuratore Speciale
- **Teleco S.r.l.: Fiorenzo Trogu**, [redacted], domiciliato per la carica presso la sede societaria in Roma, Via Rosazza n.26, nella sua qualità di Presidente del Consiglio di Amministrazione

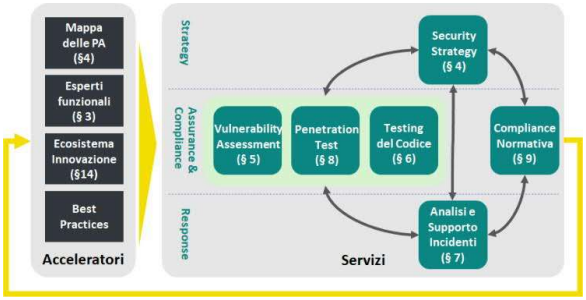
Organizzazione adottata per la distribuzione dei servizi/attività tra le aziende partecipanti. Il RTI è stato ideato con l'intenzione di mettere a disposizione delle Amministrazioni che aderiranno al presente Lotto, un **paniere esaustivo e "unico" di competenze multidisciplinari e complementari**. Le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

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

3 STRUTTURA ORGANIZZATIVA

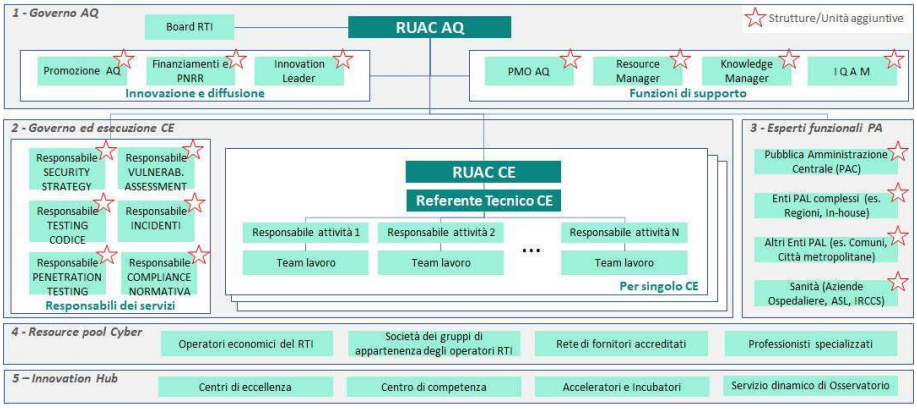
1. La **comprovata esperienza del RTI su contratti analoghi** ha consentito di progettare un modello "ad hoc" per l'erogazione dei servizi verso tipologie di Amministrazioni fortemente eterogenee **2.** Governance, flessibilità e specializzazione garantita da una **Organizzazione strutturata su 5 livelli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

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



Acceleratori: questo livello è **composto da tutti gli strumenti messi a disposizione dal RTI** che garantiscono un continuo input ai servizi dei CE in termini di valorizzazione degli esperti tematici e di **settore** (§ 3.1) e delle strutture preposte all'**innovazione** (§ 14) e di **capitalizzazione** delle best practices (§ da 4 a 9). A questo livello è manutenuta la **MappaPA** (§ 4) che garantisce, grazie a un lavoro preprogettuale di classificazione delle Amministrazioni in tipologie omogenee sulla base delle caratteristiche e dei profili di rischio delle stesse, di avere sempre a disposizione modelli predefiniti da personalizzare per ciascun CE. La MappaPA sarà pubblicata all'interno del Portale della Fornitura. **Servizi**: a questo livello il RTI ha definito un modello di interazione tra i servizi (§ da 4 a 9) che ne garantisce le sinergie, valorizzandone i risultati. Tale modello è alimentato dagli input ricevuti a livello di CE sia in termini di competenze e capitalizzazione delle esperienze, sia attraverso la guida fornita dalla MappaPA per la scelta e l'utilizzo di metodologie, tecniche e soluzioni più adatte. In un'ottica di miglioramento continuo i risultati a livello di CE costituiranno input di valore per gli Organismi di Coordinamento e Controllo.

3.1.1 Struttura organizzativa dedicata per la gestione di AQ e CE. L'organizzazione proposta dal RTI è **strutturata su 5 livelli** per garantire una **efficace governance** a livello di AQ e CE, è arricchita da figure con **competenze tematiche e dominio** che assicurano una completa copertura tecnica e funzionale, prevede il **coinvolgimento di risorse e strutture innovative** con l'obiettivo di garantire un constante **allineamento con le trasformazioni del mercato.** Le responsabilità sono distribuite tra le unità operative del RTI e sono previste figure/unità aggiuntive offerte senza alcun onere (☆) per le Amministrazioni aderenti all'AQ.



GOVERNO AQ: A questo livello risiede la governance, la programmazione e il monitoraggio dell'intero AQ. I ruoli di questo livello: **RUAC AQ** figura dirigenziale con esperienza pluriennale nella governance di programmi di trasformazione in ambito Cybersecurity. Adempie agli obblighi di cui all'Appendice 1 del CTG (par. 2.2) e assicura la guida dell'AQ garantendo, a Consip e agli Organismi di Coordinamento e Controllo (OCC), un'omogeneità di approccio su ciascun CE; definisce gli indirizzi strategici a livello di AQ e verifica l'aderenza dei singoli CE agli stessi. Presiede il Board del RTI composto da un profilo di vertice di ciascuna componente. Nelle attività il RUAC è coadiuvato dalla struttura **Funzioni di Supporto** (**FdS**) che è composta da: →**PMO AQ** (☆) Pianifica e monitora l'avanzamento complessivo dell'AQ, assicurando al contempo omogeneità di standard qualitativi (adottati a livello di CE) e di approccio nella definizione dei documenti di pianificazione e stato avanzamento lavori (SAL). Supporta operativamente il RUAC nelle attività di elaborazione della reportistica di monitoraggio dell'AQ da mettere a disposizione di Consip e OCC. →**Resource Manager RM** (☆) Gestisce centralmente il processo di staffing dei professionisti del RTI all'interno dei team di intervento sui diversi CE, individuando le professionalità più idonee per soddisfare i fabbisogni di supporto e innovazione. Gestiste a livello di AQ i processi di allocazione, ottimizzando le trasferte dei professionisti del RTI rispetto alle sedi di erogazione dei Servizi. →**Knowledge Manager KM** (☆) assicura la valorizzazione e il riuso del patrimonio di best practices e "lesson learned" acquisite durante la fornitura anche attraverso la formazione e l'aggiornamento continuo delle risorse del RTI di cui è responsabile (§ 16). →**IQAM** (☆) il RTI prevede il coinvolgimento di una figura esterna al team (Independent Quality Assurance Manager– IQAM), di profilo internazionale sui progetti più significativi allo scopo di garantire un rigido processo di quality review indipendente (Service Quality Program), che prevede sui singoli progetti previsti dal Lotto, una sistematica revisione delle attività svolte e che ha l'obiettivo di recepire e monitorare il livello di soddisfazione del cliente instaurando una relazione indipendente con esso. In staff al RUAC è prevista una ulteriore struttura di **Innovazione e Diffusione (I&D)** così composta: →**Promozione AQ** (☆) promuove la diffusione dell'AQ tramite iniziative e seminari per assicurare il massimo livello di adesione delle PA interessate e supportandole nelle fasi operative di adesione all'AQ. →**Finanziamenti e PNRR** (☆) supporta le Amministrazioni nell'identificazione di fonti di finanziamento (es. PNRR o altri fondi comunitari e nazionali) per i progetti nell'ambio dei CE. →**Innovation Leader** (☆) ingaggia sul singolo CE le strutture dell'ecosistema interno ed esterno (Innovation Hub) più idonee alle esigenze di ciascun CE per assicurare la migliore risposta in termini di soluzione innovative contribuendo all'evoluzione continua del sistema di protezione del comparto.

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

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

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

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

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

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

MODELLO DI DISTRIBUZIONE DELLE RESPONSABILITA'

Il RTI ha definito sin dalla fase di offerta una chiara assegnazione del livello di coinvolgimento di ogni componente del costituendo RTI. DRA e EYA hanno perseguito un percorso di specializzazione differente che ha portato DRA a focalizzarsi maggiormente sugli ambiti Operations e Verifiche tecniche, mentre EYA sugli ambiti Strategy e Compliance. Per tale motivo, DRA avrà maggior prevalenza sulle attività di Vulnerability Assessment, Testing del Codice, Penetration Testing e Supporto Incidenti; mentre EYA sulle attività di Strategy e Compliance. TEL (PMI Innovativa) è coinvolta nel RTI al fine di valorizzare l'innovazione nell'esecuzione su specifici servizi. Il coinvolgimento sarà nelle attività di ricerca e sviluppo funzionali ad elaborare soluzioni ed approcci metodologici innovativi, in particolare per le attività di Testing del Codice e Penetration Test in ambienti tecnologici emergenti (Cloud Computing, Big Data & Analytics, 3D User Experience, Internet of Things, Smart & Intelligent Building). Tali tecnologie potranno trovare applicazione ai servizi del Lotto 2 anche allo scopo di contribuire a qualità e innovazione dei servizi in ambito.

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

Molto Basso ○ Basso ◔ Medio ◑ Medio-Alto ◕ Alto ●

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

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

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

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

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

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

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

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

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

FASE	ATTIVITÀ	-W1	W1	W2	W3	W4
Pianificazione	Predisposizione Piano di Subentro	◆				
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	◆	◆	◆	◆	◆

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

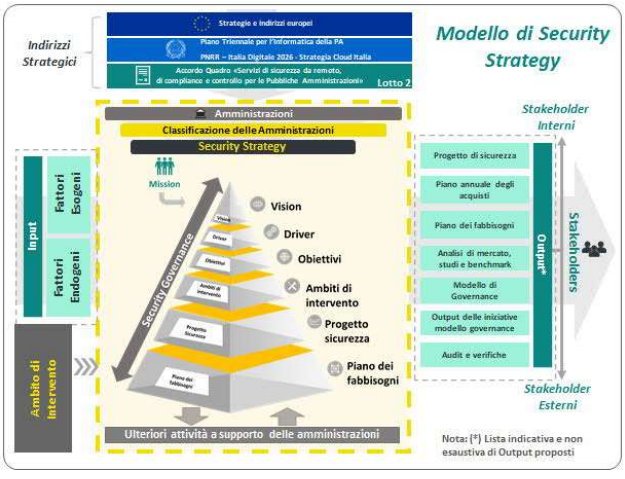
RUOLO	EFFICACIA	ADERENZA AL CONTESTO	COERENZA GENERALE	MOD. INTERAZIONE
I&D - Resp. Promozione AQ	Garantisce un coordinamento unificato su promozione e comunicazione dell'AQ	Focalizzazione e specializzazione sulle caratteristiche dell'AQ	Punto unico per le attività di marketing e business development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

4 PROPOSTA PROGETTUALE PER IL SERVIZIO "SECURITY STRATEGY"

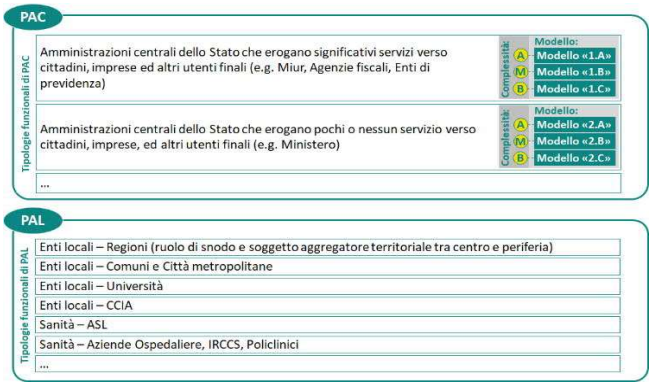
La strategia di sicurezza è l'abilitatore fondamentale che consente di individuare le azioni più appropriate per gestire i rischi di sicurezza in coerenza con le specificità delle Amministrazioni individuando le modalità con cui raggiungere i livelli di sicurezza richiesti e al contempo assicurare la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

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

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

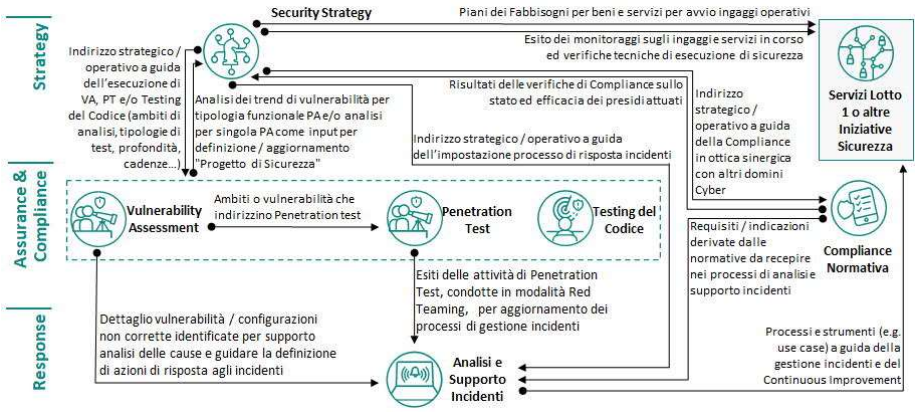


Cloud Computing, Cyber Awareness & Training, Security Operations ●**Detect**: Monitoraggio continuo di sicurezza, Incident Detection, Threat intelligence, Threat Hunting; ●**Response**: Cyber Incident Response, Investigation and Forensics ●**Recovery**: Continuità Operativa and Crisis Management, Disaster Recovery. Il valore aggiunto apportato dal RTI è l'adozione di un **approccio flessibile** in grado di supportare le Amministrazioni nella elaborazione di **PdS concreti, efficaci e sostenibili**, che si adatterà alla tipologia, al livello di complessità ed alle esigenze di protezione dell'amministrazione. A tal fine, il RTI ha sviluppato un **metodo di classificazione delle Amministrazioni** basato sulle **tipologie funzionali** integrate da una dimensione di **complessità, quest'ultima** basata su: ●numerosità dei servizi offerti a cittadini, imprese o altri utenti ●dimensione dell'amministrazione (es. dimensioni dei Comuni) ●criticità dei dati degli utenti trattati (es. Enti Sanitari vs Università) ●livello di centralità in relazione a tematiche di cooperazione ed interconnessione con le altre Amministrazioni ●contesto normativo applicabile. Sulla base di tale metodo e delle esperienze consolidate in ambito Sicurezza ICT, trasversalmente ad entrambi le classi delle PA, il RTI intende proporre l'utilizzo di specifici **modelli (prototipi) di PdS**, in termini di obiettivi ed ambiti da indirizzare, sulla base dei **profili di rischio** associati alle differenti combinazioni di Tipologia e Complessità. **(fase 1)** Il prototipo è uno strumento, differenziato in funzione delle dimensioni sopra considerate, finalizzato ad una rapida ricognizione dei presidi di sicurezza esistenti integrando, laddove disponibili, gli esiti del questionario di autovalutazione del livello di applicazione dei controlli ABSC delle misure minime di sicurezza AGID. **(fase 2)** Tale ricognizione includerà una serie di fattori determinanti per la definizione di un Progetto efficace e concreto, in particolare: ●le iniziative in essere e previste in materia di sicurezza informatica e sicurezza delle informazioni ●il modello IT, gli elementi infrastrutturali, organizzativi, applicativi esistenti e di prossima introduzione (es. PSN, evoluzione verso architetture cloud) ●Regolamenti e disposizioni organizzative interne ●specifiche minacce cyber applicabili al contesto e relativi rischi, inclusi quelli legati alla gestione dei contratti di servizio ●risk appetite, in relazione al profilo di rischio dell'Amministrazione ●ulteriori elementi, ove disponibili, quali ad esempio risultati di audit, assessment, incidenti di sicurezza. Tale approccio rappresenta un elemento preliminare e facilitatore nel disegno dei Progetti delle singole Amministrazioni e sarà personalizzato sulla base del contesto ed in particolare del livello di digitalizzazione dell'Amministrazione stessa. Nel caso **delle Amministrazioni meno complesse**, tipicamente contraddistinte da minore strutturazione dei presidi di sicurezza e limitate capacità di investimento, il valore aggiunto di questo approccio *è quello di* **rendere accessibile lo strumento di pianificazione della sicurezza ICT** (PdS)**,** grazie ad un minor effort richiesto, alle Amministrazioni stesse nella definizione degli obiettivi e degli ambiti del Progetto. Il RTI dispone dei modelli di base coerenti con le principali tipologie funzionali di Pubblica Amministrazione, con ulteriori declinazioni relative a settori specifici ed a maggiore criticità (es. il modello sviluppato per l'ambito specifico degli Enti ospedalieri). Partendo dai modelli di base, durante lo svolgimento delle attività progettuali saranno adattati/sviluppati ulteriori modelli specifici per meglio cogliere le peculiarità di ogni tipologia di amministrazione, favorendo la **logica del riuso e l'ottimizzazione conseguente dei costi**. Allo scopo di incrementare la consapevolezza delle Amministrazioni, i modelli proposti dal RTI saranno pubblicati nell'"Area Informativa" del Portale, riservata alle Amministrazioni. Sulla base delle informazioni raccolte e del Modello di Security Strategy, l'elaborazione del PdS si concretizzerà in un percorso analitico che a partire dalla **Missione** dell'Amministrazione, **(fase 3)** definirà la **Visione** strategica di sicurezza e i relativi driver. Tali driver saranno declinati **(fase 4)** in **Obiettivi** strategici, tattici e operativi, per il cui raggiungimento saranno definite **(fase 5)** specifiche iniziative correlate agli **ambiti di intervento** del PdS dell'Amministrazione. **4.1.1.1 SUPPORTO ALLA GOVERNANCE E ULTERIORI ATTIVITÀ. Supporto alla Governance** Funzionalmente a quanto sopra, il Modello proposto dal RTI prevede il disegno e la realizzazione di una Security Governance dinamica il cui valore aggiunto è quello di: ●garantire il controllo di quanto indirizzato a livello strategico ●rivalutare il PdS sulla base dei risultati ottenuti e/o delle nuove esigenze di Sicurezza ICT derivanti da eventuali evoluzioni delle normative, delle architetture, delle tecnologie e del modello IT dell'Amministrazione. Con riferimento al **disegno del modello di governance**, il RTI supporterà le Amministrazioni nella ●**(Fase 1)** formulazione di una strategia e di una architettura di monitoraggio del contesto interno ed esterno ●**(Fase 2)** definizione di una dashboard di monitoraggio del PdS dell'Amministrazione che individui e rappresenti KPI, KRI e metriche di sicurezza (*Cyber Security Dashboard*). La **declinazione operativa della governance** includerà quindi le seguenti attività: ●**Monitoraggio:** attività di verifica dell'andamento del PdS delle Amministrazioni tramite attività di reporting, analisi dei risultati, tracciatura e supporto nella gestione di eventuali problematiche di progetto ●**Controllo:** attività utili a verificare la coerenza delle iniziative del PdS rispetto alle scelte strategiche ●**Gestione del rischio:** attività volte a valutare (anche nel continuo attraverso l'utilizzo di KRI) e gestire il livello di esposizione al rischio di sicurezza garantendo il rispetto dei livelli di rischio di sicurezza ICT all'interno di soglie di tolleranza definite ●**Gestione delle classificazioni e tassonomie**: attività volte ad assicurare uniformità di classificazioni e tassonomie nei processi di sicurezza ●**Lesson learned**: attività di rielaborazione delle indicazioni strategiche funzionalmente ai dati provenienti dai singoli servizi ●**Gestione delle risorse:** attività volte ad assicurare, un utilizzo efficiente di tutte le risorse economiche e tecniche nell'ambito del PdS dell'Amministrazione in linea con quanto previsto nei fabbisogni. **Ulteriori Attività a Supporto.** Il RTI fornirà inoltre ulteriori attività di supporto consulenziale in ambito Sicurezza ICT a favore dell'Amministrazione, trasversalmente alle attività precedenti, il cui valore aggiunto è rappresentato dall'utilizzo delle migliori capacità ed esperienze similari nella definizione, coordinamento e monitoraggio di PdS , quali ad esempio: ●**Predisposizione analisi, studi e benchmark** in materia di sicurezza informatica volti a supportare le scelte di modello IT e di sicurezza dell'Amministrazione in coerenza con il processo di trasformazione digitale (nuova architetture on- premise, cloud, ibrido, PSN, etc.) ●**Consulenza tecnico-specialistica** di supporto agli stakeholder delle strutture di vertice ICT dell'Amministrazione con particolare riferimento alle valutazioni e processi decisionali ●**Promozione, affiancamento e partecipazione** a gruppi di lavoro, comitati, tavoli di coordinamento, per mettere a fattor comune elementi utili ai PdS delle singole Amministrazioni, la definizione delle strategie, l'analisi delle esigenze, la produzione di documentazione (es. politiche, linee guida) ●**Interfaccia con i provider tecnologici** con l'obiettivo di analizzare e indirizzare eventuali elementi di natura tecnologica, garantendo un efficace allineamento al PdS.



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

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



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

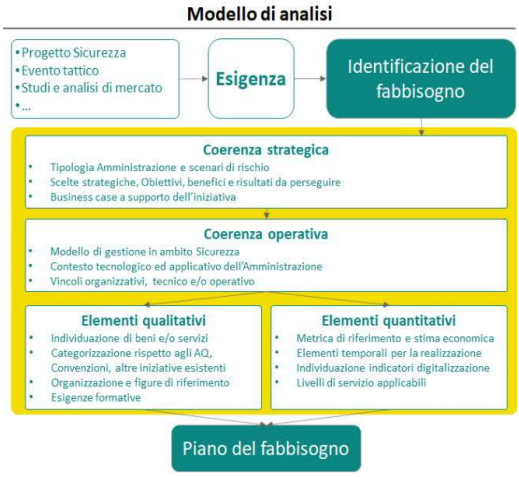
Deliverable	Contenuti esemplificativi
PdS	Documento unitario e integrato contenente la descrizione dell'insieme delle iniziative di sicurezza, nello specifico, a titolo esemplificativo e non esaustivo: ● Analisi del contesto e individuazione delle macro esigenze; ● Vision e obiettivi strategici, tattici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

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

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

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

operativi occorsi (ad esempio un incidente, una vulnerabilità), il modello proposto analizzerà le informazioni da prevedere all'interno del Piano del fabbisogno e si compone dei macro-ambiti: ● **(Fase 1) Coerenza strategica**: sulla base di obiettivi ed ambiti previsti nel PdS (§3.1.1.1), saranno valutati gli obiettivi, i benefici ed i risultati da perseguire tramite la fornitura allo scopo di garantirne il necessario allineamento con le linee strategiche dell'Amministrazione; laddove richiesto, il RTI fornirà supporto anche alla redazione di un business case della fornitura per facilitare il processo di richiesta del budget necessario. ● **(Fase 2) Coerenza operativa**: tali analisi saranno necessarie per garantire l'integrazione dei beni e dei servizi oggetto della fornitura nel modello esistente di gestione sia IT sia Sicurezza; saranno in particolare valutati il contesto tecnologico ed applicativo esistente nonché eventuali vincoli organizzativi, tecnico e/o operativo che potrebbero avere un impatto sull'adozione dei beni e/o l'erogazione dei servizi oggetto della fornitura. ●**(Fase 3) Elementi qualitativi**: tale analisi fornirà una caratterizzazione completa dei beni e servizi allo scopo di categorizzarli e prevede un supporto da parte del RTI nell'individuazione degli AQ, delle Convenzioni e di altre iniziative esistenti



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

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

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

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

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

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

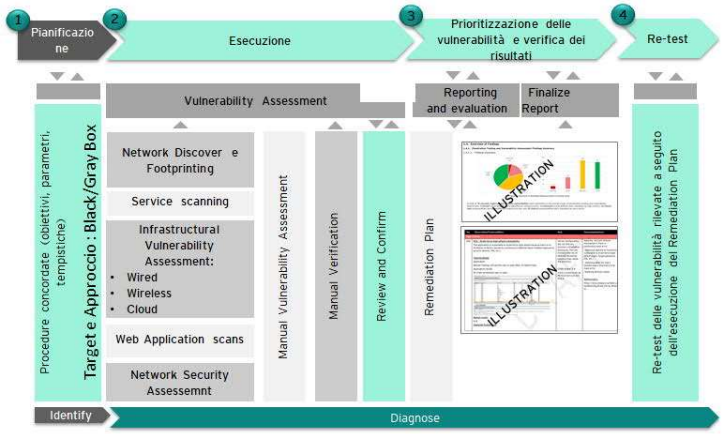
Profilo	Requisito migliorativo Generale	Requisito migliorativo Specifico
Security Principal	Nel team sarà inclusa almeno una risorsa con attestato **ITIL Foundation v3/v4 o Prince 2 Foundation/IPMA/PMI**	
Security Solution Architect		
Senior Information Security Consultant		Possesso della qualifica di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

5 PROPOSTA PROGETTUALE PER IL SERVIZIO "VULNERABILITY ASSESSMENT"

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

1. Standardizzazione del reporting e dei piani di prioritizzazione/remediation attraverso l'utilizzo di una **piattaforma centralizzata** (denominata Bug Blast) ed **indipendente dai motori di scansione** (vulnerability scanner), garantendo ripetibilità ed uniformità dei risultati **2. Metodologia per la definizione 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.).

5.1 MODALITA' DI ESECUZIONE DEL SERVIZIO. Le attività di Vulnerability Assessment (VA) forniranno evidenze di dettaglio sulle vulnerabilità riconducibili all'infrastruttura ICT e IoT/OT (es. dispositivi interconnessi impiegati nei diversi contesti di utilizzo - es. smart city, ambito sanitario, progetti open data), funzionali anche ad elaborare una *baseline* iniziale del livello di vulnerabilità e di esposizione del sistema informativo dell'Amministrazione. L'attività sarà svolta sia con strumenti automatici (continuamente aggiornati rispetto alle vulnerabilità di nuova identificazione) sia con strumenti definiti ad-hoc (es. script) sulla base della tipologia del target oggetto di analisi. Le attività saranno inoltre supportate dall'ecosistema di innovazione interno ed esterno (§ 14). Il RTI, sulla base della propria esperienza e del contesto di riferimento in cui saranno svolte le analisi di sicurezza, proporrà gli strumenti di analisi più adatti per l'esecuzione dei VA (open-source, proprietari e/o di mercato). Le attività di VA eseguite sono basate sulle metodologie OSSTMM, OWASP, PTES, NIST 800-52/53 e ISA 62443, riconosciute globalmente come standard de-facto. L'applicazione di tali metodologie garantirà risultati coerenti, ripetibili e misurabili.



Nell'ambito delle attività di VA terremo in considerazione il sempre più diffuso utilizzo delle tecnologie Cloud da parte delle 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. Le attività saranno eseguite in modalità **Black-box**, che presuppone la verifica del livello di sicurezza dei target senza alcuna credenziale di accesso (non autenticato), e **Gray-box**, ovvero verifica del livello di sicurezza dei target simulando un attaccante che possiede una parziale conoscenza dell'infrastruttura oggetto di analisi e credenziali di accesso con privilegi base (autenticato). Per l'esecuzione dei servizi richiesti dall'Amministrazione, la metodologia prevede l'esecuzione di **4 fasi progettuali**: *Pianificazione delle attività, Esecuzione dei Vulnerability Assessment, 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**, offrendo sempre un **approccio agnostico rispetto ai vendor** utilizzati per la scansione. Le informazioni che afferiscono alle attività di VA richieste saranno disponibili nel portale tramite un sistema di autorizzazione granulare e le Amministrazioni potrà accedere a tali informazioni sulla base del periodo di retention che sarà concordato di volta in volta con le stesse e comunque, salvo diversa indicazione da parte dell'Amministrazione e nel rispetto delle normative vigenti, per un periodo garantito non inferiore a 1 mese dalla fine delle attività. Tale modalità di erogazione è consigliata dal RTI, che tuttavia è disponibile ad adattare la stessa sulla base di eventuali esigenze delle Amministrazioni, concordandole di volta in volta con le stesse. **Approccio operativo.** L'approccio operativo proposto dal RTI prevede l'esecuzione di tutte le attività tecniche previste dal CTS. Si sottolinea che quanto riportato di seguito offre una vista di alto livello delle attività operative che saranno svolte dal team: ●**Pianificazione**: tale fase è fondamentale per la pianificazione delle attività di VA (tempi e orari) e per la raccolta delle informazioni necessarie all'esecuzione di verifiche di sicurezza efficaci. Nello specifico saranno eseguite le seguenti macro-attività: ▪ Identificazione degli stakeholder rilevanti ▪ Richiesta e raccolta della documentazione in ambito (es. disegni di rete, analisi funzionale, requisiti di sicurezza), nonché delle informazioni preliminari all'esecuzione dei VA (es. URL, indirizzi IP);), ▪ informazioni necessarie per identificare le normative applicabili (es. GDPR) e degli standard di sicurezza applicati dal cloud provider (es. ISO27001), ▪ Condivisione con l'Amministrazione delle metodologie, degli strumenti e delle modalità di esecuzione. La proposta di modalità di scansione sarà condivisa con l'Amministrazione in base a: criticità target, rilevanza dei target in ambito GDPR, potenziali impatti su sistemi legacy, bottleneck su alcuni sistemi/segmenti di rete, ecc. ▪ Definizione del piano di dettaglio delle attività, comprensivo di data di inizio, fine e orari di esecuzione, per definire le migliori finestre temporali per minimizzare i rischi connessi all'interruzione del servizio e/o al degrado delle performance ▪ Comunicazione all'Amministrazione degli IP delle macchine che eseguiranno i VA ▪ Esecuzione di test di raggiungibilità/accesso del target oggetto di analisi ▪ Richiesta di autorizzazione per l'avvio delle attività ●**Esecuzione**: in tale fase sono rilevate le vulnerabilità presenti per i target oggetto di analisi mediante tool automatizzati e tecniche manuali. I tool di analisi utilizzati per l'esecuzione delle scansioni automatizzate saranno opportunamente scelti e configurati (es. policy di scansione, credenziali di accesso ai tenant cloud) coerentemente con il contesto

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

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

Ambito di utilizzo	Principali strumenti
Vulnerability Assessment	● **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

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

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

VA Technical Report	Documento tecnico contenente un'analisi dettagliata e completa del livello di sicurezza, insieme a tutte le informazioni sulle vulnerabilità riscontrate (baseline), e relative azioni per mitigare o risolvere tali vulnerabilità. Il Technical Report è formato da resoconti analitici e grafici e contiene i seguenti elementi principali: ● Descrizione di dettaglio dei test di sicurezza eseguiti sui target in ambito (on premises - on cloud); ● La lista di tutte le vulnerabilità riscontrate con indicazione di: nome della vulnerabilità sulla base del CVE (Common Vulnerabilities and Exposures), livello di severità in base alla probabilità di sfruttamento (alto, medio, basso) ed all'impatto legato allo sfruttamento della vulnerabilità (alto, medio, basso per Riservatezza, Integrità e Disponibilità - RID), dettagli tecnici sulla vulnerabilità rilevata ed evidenze documentali (con eventuale supporto di immagini e tabelle) delle attività svolte (comandi eseguiti e risposte dei sistemi). **Le informazioni dimensionali** per la valutazione delle vulnerabilità e delle relative remediation sono basate sul sistema di scoring delle vulnerabilità CVSS e sono principalmente le seguenti: **vettore di attacco, complessità di attacco, privilegi richiesti, tipologia di interazione dell'utente, possibilità di propagazione, impatti su confidenzialità, integrità e disponibilità**. Ciascuna delle dimensioni citate sono valorizzate su una scala dimensionale da 1 a 10, con una sintesi finale di rischiosità che può assumere i **seguenti valori qualitativi**: critico, alto, medio o basso.
VA Remediation Plan	**Remediation plan** comprensivo delle iniziative tecniche da pianificare e svolgere per la mitigazione/risoluzione delle vulnerabilità identificate. Per ogni azione di rimedio sono fornite le seguenti **informazioni dimensionali** di dettaglio: attività da svolgere per la risoluzione delle vulnerabilità, complessità richiesta, nonché tempistiche dell'Amministrazione per l'esecuzione della stessa. Ciascuna delle dimensioni citate è valorizzata secondo le seguenti **informazioni qualitative**: tipologia di remediation (es: *R1-risoluzione completa* con azione da implementare, *R2-soluzione alternativa/compensativa/workaround*), complessità per la risoluzione tecnica della vulnerabilità (*C1-molto alto*, *C2-alto*, *C3-medio* o *C4-basso*), tempistiche di risoluzione stimate (*T1-ore*, *T2-giorni*, *T3-settimane* o *T4-mesi* con relativa proposta di pianificazione). Tali parametri sono determinati sulla base della collaborazione con i principali team operativi dell'Amministrazione impattati dalla vulnerabilità riscontrata e dall'azione di rimedio definita per la risoluzione. La determinazione di **Priorità nell'applicazione delle azioni di rimedio** è infine determinata dalla combinazione delle informazioni qualitative descritte e la **rischiosità della vulnerabilità**. Il parametro di Priorità risultante è espresso in termini di *P1-Critica*, *P2-Alta*, *P3-Media* o *P4-Bassa*.

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

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

6 PROPOSTA PROGETTUALE PER I SERVIZI "TESTING DEL CODICE"

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

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

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

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

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

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

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

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

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

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

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

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

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

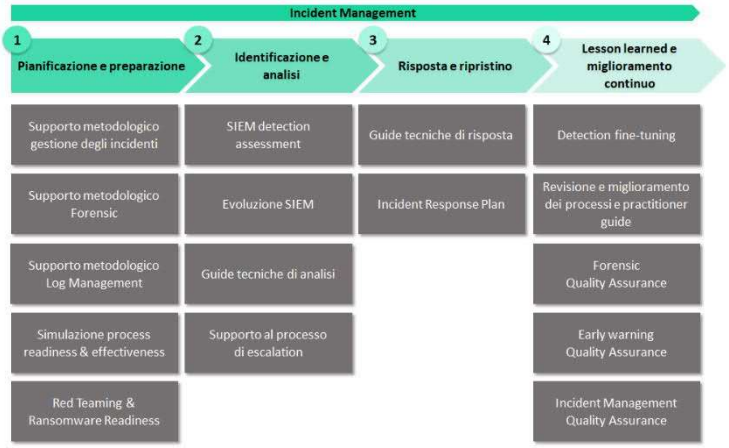
applicazioni, complessità e linguaggi di sviluppo, il tutto in **modalità trasparente per l'utente finale**. Tale modalità di erogazione è consigliata dal RTI, che tuttavia è disponibile ad adattare la stessa sulla base di eventuali esigenze delle Amministrazioni, concordandole di volta in volta con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

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

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

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

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



Il servizio di supporto all'analisi e gestione degli incidenti proposto affronta la tematica in modo olistico e multidisciplinare, in modo da promuovere il miglioramento continuo della *Incident Readiness* dell'Amministrazione attraverso elementi quali la corretta definizione dei processi, un'adeguata formazione del personale e l'ingegnerizzazione delle tecnologie di sicurezza, fondamentali per garantire nel tempo efficacia, efficienza e tempestività al servizio remoto di Incident Management erogato dal fornitore del Lotto 1 (laddove attivato) o da altre terze parti coinvolte e far fronte alla costante evoluzione degli attacchi informatici e all'incremento delle tipologie degli ambienti in perimetro (es. servizi cloud, dispositivi mobile, IoT, ecc.). Al fine di raggiungere tali obiettivi, il RTI si candida a supportare l'Amministrazione al fine di (**A**) abilitare il corretto svolgimento di ciascuna delle fasi di gestione degli incidenti attraverso attività consulenziali da svolgersi in maniera preventiva come supporto all'intero processo (analisi e progettazione) e (**B**) definire un processo strutturato di Forensic e verificarne l'efficacia (verifica). Tali attività saranno svolte in linea con i principali standard (es. ISO/IEC 27035, ISO/IEC 27002, NIST 800.61sp2), normative e linee guida di settore (es. DL 65/2018, DL 81/2021, Framework Nazionale per la Cybersecurity e la Data Protection), integrandosi inoltre con gli altri servizi del presente Lotto 2 e del Lotto 1, secondo quanto riportato all'interno del "Modello Correlazione Servizi", descritto all'interno del capitolo *Proposta progettuale per il servizio "Security Strategy"*.

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

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

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

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

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

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

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

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

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

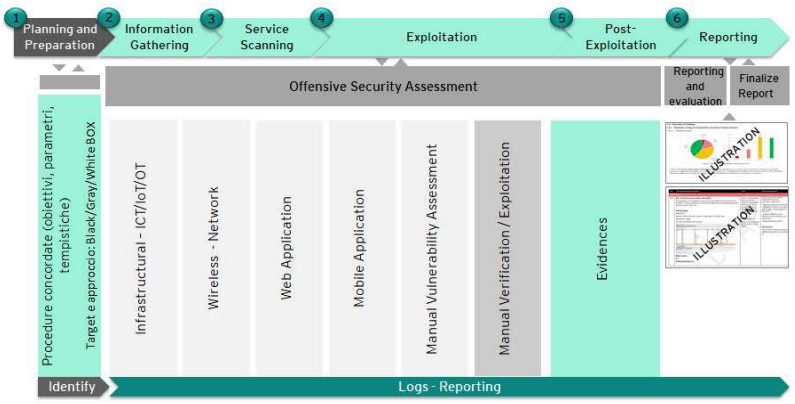
Profilo	Requisito migliorativo generale
Security Principal, Senior Security Analyst, Junior Security Analyst, Forensic Expert	Nel team sarà inclusa almeno una risorsa con certificazione **CISSP o CISM o Lead Auditor ISO 27001.**

8 PROPOSTA PROGETTUALE PER IL SERVIZIO "PENETRATION TESTING"

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

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

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



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

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

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

Ambito di utilizzo	Principali strumenti
PT Infrastrutturale	● **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

Ambito di utilizzo	Principali strumenti
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

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

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

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

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

9 PROPOSTA PROGETTUALE PER IL SERVIZIO "COMPLIANCE NORMATIVA"

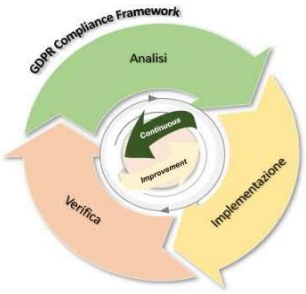
Il servizio di Compliance normativa prevede la definizione di un **Sistema di gestione della Privacy** in grado di governare **in un'ottica di lungo periodo** tutti gli adempimenti GDPR impattanti sui sistemi IT. Il RTI si impegna ad erogare le attività in ambito nel rispetto dei requisiti tecnico-funzionali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

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

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

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

9.1.1 MODALITA' DI ESECUZIONE DEL SERVIZIO E AMBITI DI INTERVENTO



Il Sistema di gestione della Privacy ha necessità di essere disegnato, analizzato, implementato, monitorato e continuamente migliorato in un'ottica anche di lungo periodo, al fine di trasformare la privacy in un **fattore abilitante** per il trattamento dei dati da parte dell'Amministrazione e garantire agli interessati (es. cittadini, utenti, dipendenti dell'Amministrazione) la protezione dei dati personali. A tale scopo, il RTI utilizzerà, per guidare lo svolgimento delle attività, il **GDPR Compliance Framework (GDPR CF)**. Tale strumento propone una metodologia per la definizione e mantenimento del sistema privacy ed è caratterizzato da un ciclo di 4 fasi: a) Analisi; b) Implementazione; c) Verifica; d) Continuous Improvement. Quest'ultima fase è abilitata dal **Privacy Maturity Model (PMM)**, ovvero uno strumento in grado di intercettare nel continuo, i punti di forza e di miglioramento del Sistema di gestione della privacy esprimendo lo stato di maturità e identificando in modo dinamico le aree di intervento. L'utilizzo del GDPR CF, oltre a mettere a disposizione un **set esaustivo di strumenti automatici**, potrà, in funzione delle esigenze progettuali, essere supportato da un **prodotto software integrato che consente di gestire il Sistema Privacy in modalità condivisa e collaborativa tra tutti i soggetti interessati** (es. DPO, Privacy Officer, IT, Sicurezza, Risorse Umane, Acquisti). In entrambi i casi saranno garantite tutte le funzionalità sotto descritte. Con particolare riferimento agli strumenti di analisi e template, in analogia al servizio di Security strategy, il framework prevede **modelli differenziati per tipologia e complessità delle amministrazioni considerate** (in tal modo, considerando la completa copertura dei requisiti privacy, i template/checklist saranno più o meno articolati a seconda che si consideri una grande o una piccola amministrazione).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

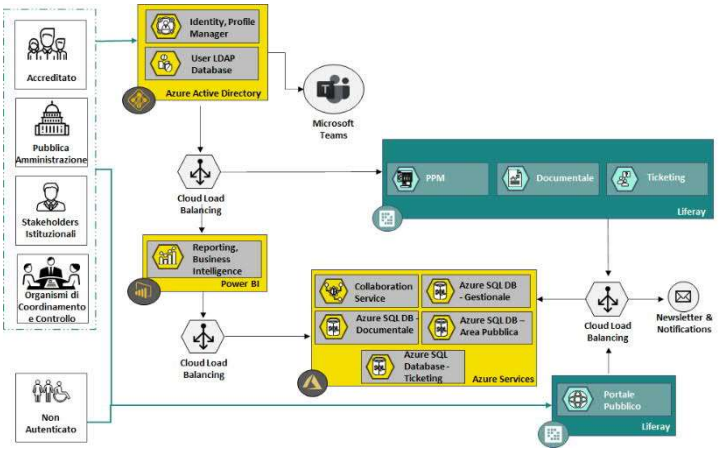
10 PORTALE DELLA FORNITURA

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

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

10.1 SOLUZIONI TECNOLOGICHE E FUNZIONALITÀ PROPOSTE

10.1.1 LA TECNOLOGIA Le componenti previste per il Portale della Fornitura possono essere raggruppate in 3 tipologie di layer: ●**Layer logico**: rappresenta la vista di tutte le funzioni, servizi e processi di business verticali e trasversali per la gestione dell'intera fornitura ●**Layer tecnologico**: contiene gli strumenti e piattaforme tecnologiche atte a supportare ed erogare tutte le funzionalità e i servizi del layer logico. Il RTI intende integrare i migliori prodotti di mercato, certificati dai Magic Quadrant di Gartner, per la gestione delle componenti di PPM, Comunicazione, Reporting, Marketing e Customer Satisfaction, quali: LIFERAY è la piattaforma di portali Open Source, leader mondiale, che offre funzionalità di pubblicazione e gestione di contenuti Web. Presenta un'architettura orientata ai servizi e compatibilità con tutte le principali infrastrutture IT; Microsoft Teams è una piattaforma di comunicazione unificata che combina in un unico workspace chat di lavoro, email, riunioni video, gestione documenti (compresa la collaborazione istantanea tra più utenti su documenti); Power BI è una piattaforma software di Data Analytics e Business Intelligence (BI) che offre funzionalità di reporting, data integration, OLAP services, information dashboards, data mining e risorse ETL; hotjar consente: → di progettare e realizzare survey online su cluster di utenti selezionati, analizzando più variabili in relazione a servizi/processi/percezioni; → di monitorare le conversazioni sia su canali non-owned (forum, blog, pagine Facebook appartenenti ad altre organizzazioni, ecc.) che su canali proprietari (es. portale servizi dell'Amministrazione); → di effettuare sentiment analysis; → la disambiguazione e l'auto-apprendimento basato su un training della piattaforma che consente di migliorare l'accuratezza della selezione fatta in automatico; → il real time tracking e l'analisi delle conversazioni; → sondaggi coinvolgenti sfruttando grafiche accattivanti e icone di gradimento; → di integrarsi con piattaforme per tenere sotto controllo le valutazioni e analizzarne il cambiamento nel tempo.

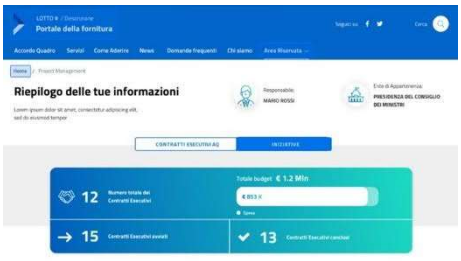


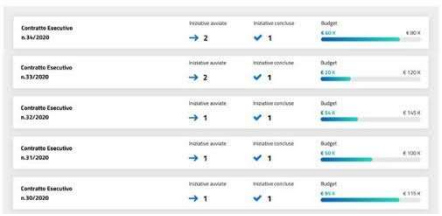
●**Layer architetturale:** rappresenta la panoramica infrastrutturale del Portale con lo scopo di proporre una soluzione moderna utilizzando le tecnologie più avanzate presenti sul mercato. In particolare, la soluzione consente attraverso un componente di tipo IDaaS (Identity-as-a-Service), inclusa in Office 365, quale Azure Active Directory, di centralizzare il processo di autenticazione in modo sicuro costituendo un meccanismo di Single Sign-On (SSO). L'utente, in funzione del profilo assegnato, viene autorizzato all'accesso a specifiche funzionalità e servizi erogati sia in ambienti SaaS, sia in IaaS ospitati su macchine virtuali Windows. Tali ambienti sono adeguatamente protetti seguendo i principi di progettazione della sicurezza cloud e le best practices dei vendor coinvolti (es: MS Azure), con il fine di garantire la riservatezza, integrità e disponibilità delle informazioni. L'infrastruttura è inoltre protetta da un servizio continuativo di monitoraggio della sicurezza e di gestione degli incidenti informatici focalizzata a rilevare eventuali minacce cyber e coordinare le azioni di mitigazione ed eradicazione. La soluzione, **interamente modulare**, consente al RTI di poter introdurre, durante l'erogazione dei servizi, componenti migliorativi, principalmente *Open Source* nel rispetto delle linee guida AgID, in grado di garantire una costante qualità del servizio. Il portale della fornitura metterà a disposizione un'interfaccia API in grado di integrare, attraverso l'ausilio dei più comuni standard di comunicazione (SOAP e/o REST), eventuali sistemi già in uso dalle PA aderenti all'AQ, come previsto da capitolato, consentendo l'adozione di modalità di lavoro collaborativo e l'uniformità dei flussi di lavorazione. Infine, grazie all'utilizzo di componenti e prodotti di tipo *Cloud-Based,* **verrà garantito un elevato livello di servizio e un'adeguata scalabilità** in funzione degli utenti che usufruiscono dei servizi esposti. Il RTI garantisce il rispetto dei requisiti tecnico-funzionali specificati nel CTS circa le modalità di integrazione degli strumenti con il Portale della Fornitura. **10.1.2 LE FUNZIONALITA'** Il Portale proposto si compone di diverse componenti logiche, di business e tecnologiche supportate da appropriate misure per garantire la sicurezza e la protezione dei dati. Il Portale si rivolge a una molteplicità di attori, ciascuno con differente visione e scopo di fruizione. Per questo motivo a ogni profilo di utenza sono dedicate specifiche Aree, funzionalità e strumenti. Le ***PA che intendono aderire all'Accordo Quadro*** possono approfondire le modalità di adesione consultando le informazioni incluse nell'area pubblica del Portale e, se interessate, possono accedere ad un'area informativa ad hoc contenente la documentazione ufficiale – normativa, tecnologica e operativa – per l'AQ nonché una guida alla stima utile a valutare la previsione di spesa generata dall'attivazione di un Contratto Esecutivo. Le ***PA che hanno aderito e sono accreditate***, insieme ai rispettivi Fornitori, possono accedere al Portale per

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

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

Il portale è organizzato secondo le seguenti aree, la cui rappresentazione esemplificativa in tabella prevede profili e politiche di accesso che saranno da concordare con Consip e AgiD in fase di attivazione: ● **AREA COMUNICAZIONE** (funzionalità ad accesso pubblico): L'***Area Comunicazione*** è accessibile a tutti gli utenti. Tramite l'Home Page del Portale (Area Comunicazione) vengono messi a disposizione contenuti quali: news inerenti alle Pubbliche Amministrazioni, l'iter di adesione all'Accordo Quadro, aggiornamenti sulle evoluzioni della PA per i cittadini e le imprese. Le Pubbliche Amministrazioni che vogliono valutare la possibilità di adesione all'Accordo Quadro possono consultare gli "step" previsti per l'accreditamento e cercare le risposte alle domande più frequenti, piuttosto che comunicare il proprio interesse ad avviare un Contratto Esecutivo. La dimostrazione di interesse avviene secondo un processo strutturato che permette di identificare univocamente la Pubblica Amministrazione che fa richiesta ●**AREA INFORMATIVA** : Area nella quale sarà possibile: → esaminare documenti inerenti i servizi previsti dall'Accordo Quadro (con descrizione puntuale degli stessi – **catalogo servizi**) e i modelli operativi previsti dalla fornitura; → consultare i **modelli (prototipi) di Progetto di Sicurezza** (§4.1.1); → confrontarsi con una guida alla stima per visualizzare la previsione di spesa legata ai servizi dell'Accordo Quadro. ●**AREA PROJECT MANAGEMENT:** L'**Area Project Management** è dedicata alla gestione dei singoli Contratti Esecutivi. È organizzata in modo da fornire alle Amministrazioni una visione di insieme sullo stato delle attività e la possibilità di governare ciascun servizio attivato. Nell'Area di Project Management è possibile gestire il workflow dei deliverable di fornitura, consultandone quindi il relativo stato di approvazione. ●**AREA COLLABORAZIONE E MONITORAGGIO:** L'**Area Collaborazione e Monitoraggio** permette agli Stakeholder Istituzionali, a Consip e agli Organismi di Coordinamento e Controllo (OCC), in virtù del ruolo specifico, di disporre di un quadro univoco sull'Accordo Quadro e sull'andamento delle attività. La rappresentazione individuata è **immediata e intuitiva**, con uno stile di comunicazione efficace. L'Area è organizzata in macro-tematiche di riferimento che permettono un approfondimento per categoria di report. Ogni categoria di report esposta potrà essere esplosa per fornire un monitoraggio di dettaglio sull'avanzamento delle varie progettualità e per avviare un'analisi sugli **indicatori di digitalizzazione**: **indicatori generali**, suddivisi a loro volta in **indicatori quantitativi**, volti a misurare dati quantitativi come riduzione di tempi e spesa, **indicatori qualitativi**, che permettono di misurare il livello di qualità della Fornitura in modo da identificare eventuali azioni contrattuali da intraprendere, ed **indicatori di collaborazione e riuso**, dedicati invece alla misurazione degli elementi di riuso; un **indicatore di progresso** dell'intervento ottenuto attraverso la realizzazione dell'Ordinativo di Fornitura, volto a calcolare il grado di mappatura di ciascuna classe di **controlli ABSC** (Agid Basic Security Control). **Per le singole PA aderenti all'Accordo Quadro il monitoraggio sarà relativo ai soli servizi attivati e relativo all'andamento degli stessi.** ●**AREA OSSERVATORIO:** L'Area Osservatorio è finalizzata alla presentazione di una **reportistica dedicata ai dati relativi alla qualità e alla sicurezza sui servizi erogati presenti in AQ**, consentendo agli OCC e a Consip di svolgere le proprie funzioni di monitoraggio. Tutti i report saranno prodotti mensilmente in modo automatico ed estraibili a richiesta.

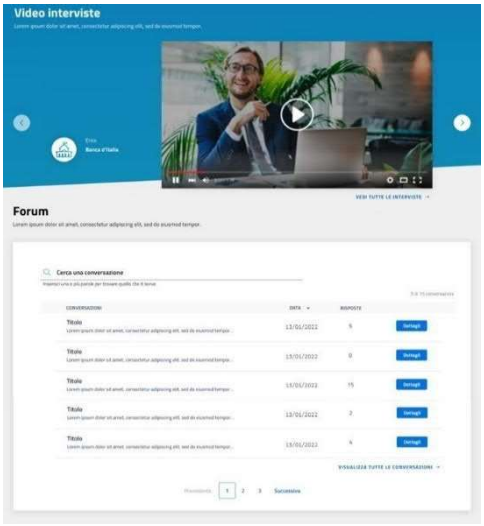




10.2 STRUMENTI DI ANALISI DEI DATI E REPORTING Nell'*area* riservata del Portale è possibile consultare, all'interno di un cruscotto centralizzato, i dati relativi all'Accordo Quadro e ai Contratti Esecutivi in termini di economics, iniziative e servizi avviati e andamento dei servizi stessi. Tali funzionalità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

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

10.3 SOLUZIONI, PROCESSI E STRUMENTI DI COMUNICAZIONE E DI COLLABORAZIONE IN CHIAVE "SOCIAL" Il Portale della Fornitura da spazio alla creazione di una **solida rete di comunicazione e collaborazione**: → risulta aperto ad acquisire dati dagli utilizzatori stessi, da altri portali di forniture concomitanti e dagli open data condivisi dalle Pubbliche Amministrazioni sul sito *dati.gov.it*.; → integra diversi strumenti di comunicazione, come tool di messaggistica broadcast verso Amministrazioni e newsletter, quali ad esempio la Privacy Highlights (§9.1.1), dedicata alle principali novità legislative e avvenimenti privacy; → favorisce l'interazione tra cittadini, imprese e PA; → garantisce trasparenza, partecipazione e collaborazione. I meccanismi e i processi di comunicazione e collaborazione con le Amministrazioni contraenti saranno effettuati attraverso il Portale, in linea con quanto riportato nella Procedura di Coordinamento Generale e nelle Procedure di Coordinamento specifiche per ogni Contratto Applicativo, come riportato nella Soluzione Organizzativa**. 10.3.1 AREA COLLABORAZIONE E MONITORAGGIO** Come strumento di **Collaborazione e Comunicazione**, all'interno della pagina "Area Collaborazione e Monitoraggio" è presente una sottosezione **Forum** che permette a tutte le PA aderenti di visualizzare e interagire nelle conversazioni più recenti in merito a diverse categorie (quali ad esempio "Attivazione nuova iniziativa", "Gestione anomalie", "Varie"), con **funzione di ricerca ed evidenza della preview della conversazione**, dell'Ente/Nome utente che ha avviato la stessa e del numero di risposte; la sottosezione può scorrere in modo da visualizzare tutte le anteprime così come presentate e in ordine cronologico; cliccando su una delle conversazioni si accede alla relativa pagina nella quale è possibile interagire con altri utenti utilizzando un servizio di messaggistica; cliccando invece su "Forum" si accede ad una pagina dedicata che permette anche l'apertura di un nuovo thread o la gestione dei filtri per una migliore visualizzazione delle discussioni già aperte. Tra gli ulteriori strumenti in chiave "Social" il RTI propone una Piattaforma di **Digital Storytelling**, fruibile sempre nella pagina "Area Collaborazione e Monitoraggio" per consentire alle Amministrazioni che lo desiderano, secondo le proprie specifiche esigenze, di condividere con altre Amministrazioni e/o Stakeholder le Lesson Learned raccontando in un breve video oppure in un webinar le caratteristiche peculiari dei progetti seguiti con il RTI, promuovendo il riuso e le attività di comunicazione e collaborazione. La Piattaforma ha a disposizione un'intuitiva interfaccia grafica che permette di selezionare le iniziative suddivise anche per tipologia, Ecosistema AgID ed indicatori di Digitalizzazione. **10.3.2 COLLABORAZIONE IN CHIAVE "SOCIAL"** La soluzione proposta per la collaborazione all'interno dei Team di Progetto impegnati sui Contratti Esecutivi, tenendo conto delle possibilità di utilizzo delle PA che hanno aderito all'AQ, è lo strumento **Microsoft Teams**, volto a ottimizzare in tutto e per tutto la produttività. È un prodotto che unifica i diversi canali di comunicazione (E-mail, Team meeting, chat) e permette a tutti gli stakeholders (in locale o da remoto) di collaborare e aumentare la produttività dei diversi deliverables della fornitura in tempo reale e su diversi dispositivi. Gli utenti riescono ad avere tutto a portata di mano: file condivisi tra tutto il team; chat; *Apps* scelte come Add-In utili per la gestione del progetto (Planner, PMO, Power BI, SharePoint, Flow, etc..); pianificazioni di riunioni; e altre funzioni utili.



11 MIGLIORAMENTO SOGLIE INDICATORI DI QUALITA' – RLFN – Rilievi sulla fornitura

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

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

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

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

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

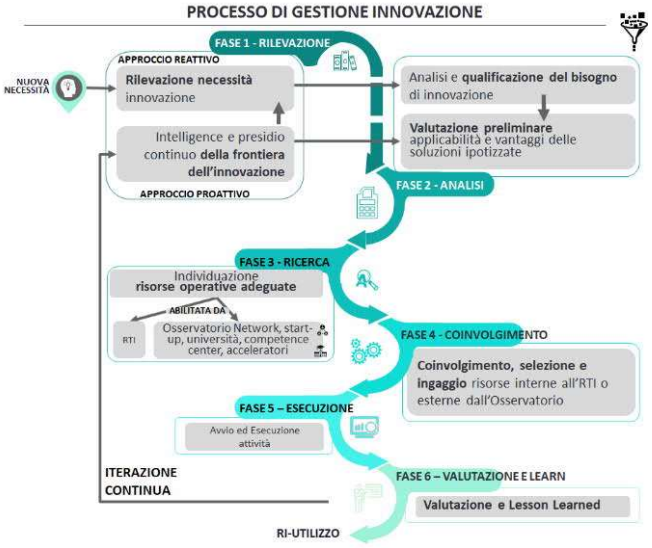
14 INNOVAZIONE

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

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

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

Ricerca) di Innovazione che rappresentano nel complesso l'**Innovation Hub** descritto in precedenza (§ 3.1.1), funzionali a garantire: 1)**Innovazione dei processi/servizi**, attraverso ●attività di **Ricerca e Sviluppo** promosse ed eseguite dalle unità operative dedicate all'innovazione di **DRA ed EYA** e delle capacità della **PMI Innovativa Teleco Srl**, nonché della **Fondazione Bruno Kessler**, Ente di Ricerca specializzato in cybersecurity che il RTI potrà coinvolgere nell'ambito di una collaborazione continuativa ●**Centri di competenza** come **Deloitte Officine Innovazione** che promuove la cultura dell'innovazione e fornirà al RTI ed alle Amministrazioni nuovi servizi per lo sviluppo e il consolidamento delle iniziative di innovazione, con focus sulle tecnologie utili per la trasformazione del business (RPA, AI, canali digitali, Cloud) e la sua protezione ●**Centri di eccellenza di OT/IoT Security** specializzati nell' attività di analisi, sviluppo e test di sicurezza. 2)**Innovazione dei prodotti/tecnologie e relativi acceleratori**, come **l'EY Funding4Innovation** o **Deloitte Switch2Product (in collaborazione il PoliHub – Politecnico di Milano)** che definisce strategie di Innovazione in linea con le opportunità di finanziamento per innovazione, trasformazione digitale, Health 4.0 (PNRR, Horizon 2020, PON e POR, fondi europei, nazionali e regionali) e guida startup e scale-up nell'accesso ai finanziamenti e nello sviluppo di soluzioni prototipali da integrare nel business aziendale. 3)**un servizio dinamico di Osservatorio di startup, acceleratori e competenze** in ambito cybersecurity abilitato da numerose iniziative come B Heroes (programma per l'innovazione rivolto in particolare alla promozione di giovani imprese), Premio EY Startup dell'anno (riconoscimento di EY al fine di dare spazio e visibilità a personalità giovani e brillanti che sono riusciti a dar vita ad un'impresa), Premio Marzotto (competizione che premia un'idea imprenditoriale in grado di generare un impatto economico - sociale positivo), Open Italy Startup Accelerator (contest che ha l'obiettivo di favorire la collaborazione tra grandi imprese, Startup italiane/PMI e abilitatori d'innovazione), al fine di fornire, sulla base di cambiamenti ed evoluzioni del mercato, le migliori soluzioni cyber in termini di innovazione.



14.2 AMBITO DI INTERVENTO E VALORE AGGIUNTO APPORTATO.

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

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

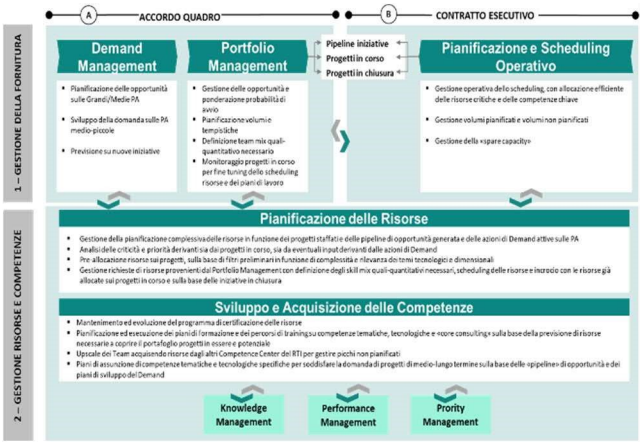
Deloitte/EY/ Teleco/FBK	**Osservatorio Privacy** finalizzato a recepire ed analizzare tempestivamente l'evoluzione normativa relativamente ai temi Privacy, Provvedimenti del Garante Privacy, opinion del EDPB, ecc. che possono avere impatto sull'Amministrazione. Tale rilevazione è garantita dall'utilizzo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

14.3 MODALITÀ ORGANIZZATIVE DEL COINVOLGIMENTO. Per garantire un **elevato livello di innovazione nell'erogazione dei servizi di gara**, il RTI propone un processo di **Gestione dell'Innovazione** che valorizzi tutti gli elementi distintivi e di unicità del RTI stesso, in termini di **modalità organizzative** utili a facilitare la collaborazione di tutte le risorse previste nella soluzione organizzativa, sia con ottica di **efficiente gestione interna che interazione esterna verso le Amministrazioni,** strutturato su un approccio ciclico (continuous monitoring). Si riportano di seguito le fasi che compongono il processo di gestione dell'innovazione ●**Fase 1**: Rilevazione dell'esigenza sulla base di un duplice approccio. ***Reattivo***: a fronte di una richiesta ricevuta. ***Proattivo***: attraverso attività di monitoraggio e presidio continuo della frontiera dell'innovazione. ●**Fase 2:** Analisi dell'esigenza di innovazione e valutazione dell'applicabilità delle soluzioni ipotizzate. ●**Fase 3**: Individuazione delle risorse operative adeguate. ●**Fase 4**: Coinvolgimento delle risorse individuate. ●**Fase 5**: Avvio ed Esecuzione attività. ●**Fase 6**: Valutazione e Lesson Learned. Per meglio rappresentare le modalità organizzative del coinvolgimento delle strutture e degli operatori selezionati, il RTI propone una modalità di risposta attraverso **l'Ecosistema Interno**, volto ad indirizzare le esigenze attraverso l'utilizzo di soluzioni innovative interne al RTI, e l'**Ecosistema Esterno**, funzionale a intercettare soluzioni attraverso l'osservazione di trend, soluzioni e strumenti innovativi di mercato**. Ecosistema interno:** a valle della rilevazione dell'esigenza, le strutture interne al RTI saranno tempestivamente attivate dal RUAC CE o dal Referente Tecnico CE, per il tramite dell'**Innovation Leader** (§ 3.1.1.), secondo il seguente approccio: 1) **ricerca delle competenze** interne al RTI necessarie a soddisfare l'esigenza espressa dall'Amministrazione, ottimizzando le tempistiche di avvio delle attività; 2) **selezione del team**, condivisione/approvazione da parte dell'Amministrazione; 3) **integrazione delle competenze** individuate nel team e avvio attività. **Ecosistema esterno:** sulla base di un'analisi proattiva degli Osservatori o nel caso in cui sia opportuna una sinergia tra le competenze/soluzioni interne al RTI e di mercato, eventuali ulteriori Startup e PMI innovative saranno ingaggiate secondo il seguente approccio: 1) **preselezione di un cluster** che include tipicamente fino a 10 operatori (in funzione dell'aderenza delle soluzioni proposte rispetto all'esigenza di innovazione ed al contesto dell'Amministrazione, ad esempio operatori con caratteristiche di prossimità geografica e attinenza alla tematica innovativa di interesse); 2) **valutazione e selezione di un massimo di 2-3 operatori** (short list) per la definizione di prototipi e/o lo sviluppo di soluzioni-pilota.

Ciascun operatore sarà valutato, in particolare, in funzione di appositi criteri (es. innovatività della soluzione offerta, funzionalità e servizi offerti, radicamento sul territorio, referenze PA ed extra PA, valore economico), opportunamente prioritizzati in coerenza con il contesto dell'Amministrazione coinvolta; 3) **selezione** della struttura/operatore più idonea. Successivamente sarà effettuata l'attivazione della struttura/operatore selezionato secondo modalità e tempi concordati di concerto con l'Amministrazione. Le **tempistiche di ingaggio** dell'**ecosistema interno**, essendo basate sui soggetti già parte del RTI (vedi PMI Innovativa) e/o vincolate da accordi di collaborazione già stipulati (ad esempio Ente di ricerca), seguono le **tempistiche di evasione** dei servizi. Il completamento delle fasi 1-3 dell'**ecosistema esterno**, avviandosi già nella fase di definizione dei fabbisogni, rispetterà le tempistiche di ingaggio previste per ciascun servizio.

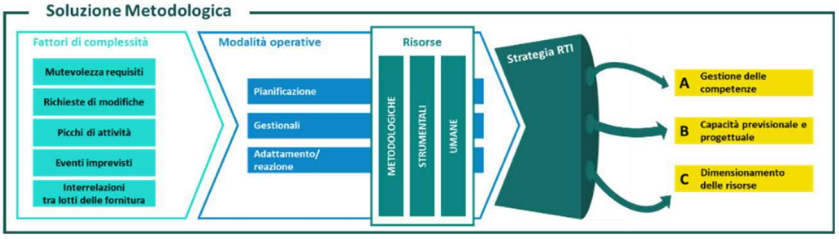
15 FLESSIBILITA' DELLE RISORSE

La variabilità delle esigenze, dei requisiti e dei possibili contesti tecnologici e gestionali rappresenta una peculiarità dell'ambito della Pubblica Amministrazione ben nota alle aziende del RTI, che **erogano da diverso tempo servizi in modalità similare** e per le quali tale complessità rappresenta una modalità di lavoro "**business as usual**". In questo ambito, **il modello organizzativo ed operativo** adottato dal RTI per la gestione flessibile di risorse si basa su: ● **la comprovata esperienza** maturata dalle aziende del RTI: ogni anno sono gestiti in media più di 2000 progetti con caratteristiche comparabili con i programmi previsti dal CTS, anche in termini di estemporaneità nell'attivazione e variabilità dei requisiti; ● la **capacità previsionale** sui tempi d'attivazione dei progetti, basata sui progetti suddetti già condotti, che consente di mobilitare le risorse con tempi medi inferiori ai 15 giorni; ● la possibilità di far leva su un considerevole **bacino di risorse interne distribuito geograficamente** che è costituito per i temi di Cyber Security da più di 500 risorse in Italia e 3000 in EMEIA**.** Queste sono supportate sul territorio nazionale da **3 Centri di Competenza** (Milano, Roma e Bari)**, 1 Centro di Delivery** (Bari)**, 2 Cyber Intelligence Center** (Milano e Roma) e da una rete di più di 500 consulenti tra fornitori accreditati e professionisti altamente qualificati ed accuratamente selezionati. La gestione della flessibilità operativa del RTI si basa sull'interazione tra (vedi figura): A) processi operativi di gestione dell'Accordo Quadro e B) processi di attuazione dei progetti dei Contratti Esecutivi (CE); e tra 1) gestione della Fornitura nel suo complesso e 2) gestione delle risorse e delle competenze all'interno delle aziende. Le caratteristiche del modello organizzativo sono: ● **Gestione proattiva della Demand.** L'approccio del RTI è primariamente proattivo e mira a implementare un processo di gestione della Demand robusto, che riduca le esigenze di gestione e mitigazione dei rischi a

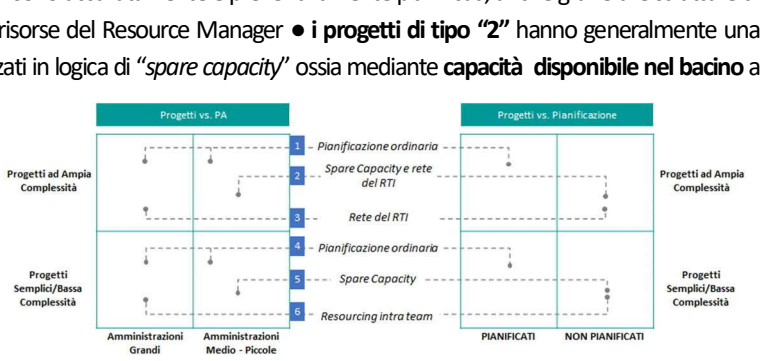


posteriori e limiti la numerosità di risposte reattive alle esigenze e ai problemi imprevisti. ● **Gestione del Portfolio Management.** L'azione strutturata del PMO AQ, di concerto con i RUAC CE, nonché il recepimento di richieste provenienti dalle Amministrazioni, consentono di definire le opportunità,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

15.1 DISPONIBILITÀ E TEMPESTIVITÀ DI ALLOCAZIONE DELLE RISORSE PROFESSIONALI L'approccio per garantire - in modo **strutturato** e **proattivo** – la **disponibilità e tempestività delle risorse** tiene conto di una serie di fattori di complessità quali: la **necessità di erogare nuovi progetti, più progetti in contemporanea verso la stessa Amministrazione o più Amministrazioni** dislocate diversamente a livello geografico, **variabilità dei requisiti, richieste di modifiche** pianificate o estemporanee, **picchi di attività** ed **eventi imprevisti**. A tale complessità, il RTI risponde con: ● **Modalità operative di pianificazione** volte a realizzare tutte quelle azioni interne al RTI che **riducono il rischio di progetti estemporanei e picchi di attività**; ● **Modalità operative gestionali**, che includono le **azioni atte a gestire le possibili variazioni del contesto**, in termini di nuovi progetti, variazione dei requisiti dei progetti esistenti, esigenze non pianificate e contrazione dei tempi che impattano sugli interventi in corso e che richiedono una revisione della pianificazione delle attività e delle risorse; ● **Modalità operative di adattamento e reazione**, ossia azioni forti e veloci di contenimento e ripristino dei livelli standard di erogazione dei servizi che limitano gli impatti sulla normale esecuzione delle attività. Tali modalità operative sono abilitate dall'utilizzo di specifiche risorse **metodologiche**, orientate alla gestione dei rischi, da risorse **strumentali,** che supportano i processi di pianificazione, e da risorse **umane,** selezionate dal bacino a disposizione del RTI, per garantire al RTI l'apporto di adeguato know-how e di background di esperienze. Il RTI propone quindi una specifica **strategia di flessibilità nella gestione delle risorse** incentrata sui seguenti elementi: A) **Gestione delle competenze**: per garantire la disponibilità delle risorse, il RTI adotta un processo centralizzato di selezione delle risorse affidata al **Resource Manager** che si avvale di una **Mappa delle Competenze,** costantemente aggiornata, per individuare risorse con skill adeguate e conoscenza del contesto. La disponibilità di un quadro di insieme di tutte le competenze richieste dalla Fornitura e la **ridondanza delle skill sul gruppo di lavoro**, ottenuta grazie alle azioni di formazione, abilita la possibilità di disporre di **risorse qualificate ed attivarle tempestivamente** sulla base delle specifiche richieste delle Amministrazioni**.** Per garantire la flessibilità nella gestione e nell'inserimento delle risorse, il RTI propone un modello operativo T-Shaped. Tale approccio interdisciplinare è applicato all'interno di tutti i servizi e comprende lo sviluppo di: → **competenze verticali**: la singola risorsa è specializzata in un ambito di riferimento; → **competenze orizzontali**: la stessa risorsa approfondisce progressivamente anche altre tematiche affini al proprio ambito di riferimento, fungendo da possibile risorsa aggiuntiva in caso di picco che richieda le stesse competenze. B) **Capacità previsionale e progettuale**: comprende tutte le azioni realizzabili al fine di: ● **Preventivare l'avvio delle nuove progettualità** grazie sia alla capacità del RTI di monitorare l'evoluzione del contesto di business, normativo e tecnologico, sia all'analisi costante del flusso di progetti già attivati nell'ambito dell'AQ. ● **Stimare l'effort e le competenze necessarie per gestire la domanda** sulla base delle esperienze progettuali già svolte ed individuare, già in fase di pianificazione**,** ogni elemento che potrebbe generare un effort diverso da quanto previsto. C) **Dimensionamento delle risorse**: la disponibilità delle risorse sui progetti è garantita da un processo strutturato di dimensionamento che prevede: ● l'identificazione, sulla base delle esigenze rilevate, delle figure professionali da impiegare sui singoli CE con le relative competenze; ● l'analisi del bacino di disponibilità delle risorse da cui verranno selezionate quelle che comporranno i Team di lavoro; ● l'aggiornamento del bacino di disponibilità in funzione degli interventi attivati; ● il dimensionamento/ridimensionamento dei Team. L'accurato processo di gestione delle competenze, capacità previsionali ed una solida metodologia di dimensionamento delle risorse in funzione delle attività consente di **efficientare l'impiego** delle risorse e garantirne la **tempestività nell'allocazione** sulle singole progettualità.



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



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

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

16 AGGIORNAMENTO DELLE RISORSE PROFESSIONALI

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

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

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

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

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

17 ASSUNZIONE DELLE RISORSE PROFESSIONALI

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