CLASSIFICAZIONE DEL DOCUMENTO: CONSIP PUBLIC

ALLEGATO 5

CAPITOLATO TECNICO

Gara a procedura aperta ai sensi del D.Lgs. 50/2016 e s.m.i., per l'acquisizione dei Security Consulting Services della Corte dei conti – ID 1828

consip

INDICE

1 INTRODUZIONE

Il presente Capitolato descrive gli aspetti tecnici relativi alla fornitura dei Security Consulting Services necessari alla progettazione e al miglioramento continuo dell'ambito IT security della Corte dei conti (nel seguito indicata per comodità con CdC).
Il Committente ha inteso organizzare la presente iniziativa di acquisizione al fine di rispondere in modo efficiente e flessibile alle esigenze attuali e future della CdC in tema di Sicurezza IT, sia da un punto di vista tecnologico che progettuale.

Tutte le prescrizioni contenute nel presente Capitolato tecnico rappresentano requisiti minimi della Fornitura.

2 DEFINIZIONI ED ABBREVIAZIONI

Salva diversa esplicita indicazione, ai termini seguenti e riportati in ordine alfabetico viene attribuito, ai fini del presente documento, il significato di seguito indicato:

- **Amministrazione:** indica la Corte dei Conti, "Cdc" ;
- **Capitolato tecnico**: indica il presente documento;
- **Committente**: SOGEI - Società Generale d'Informatica S.p.A.;
- **Data di Attivazione**: primo giorno lavorativo utile, successivo alla data di approvazione del Piano di Lavoro, da parte della Committente/Amministrazione, come indicato al paragrafo5.4;
- **Fornitura**: indica, nel suo complesso, l'erogazione dei servizi oggetto del presente Capitolato tecnico;
- **Fornitore/Impresa/Società**: indica l'aggiudicatario della Fornitura;
- **Piano di Lavoro**: indica il documento di pianificazione dei Servizi Continuativi;
- **Proposta Tecnico Economica (PTE)**: indica il documento di pianificazione dei Servizi On Demand;
- **Resoconto Attività** : indica il documento di consuntivazione dei servizi oggetto della Fornitura.

2.1 Acronimi

- **GP:** Giorno/i Persona;
- **IaaS:** Infrastructure as a Service;
- **MSSP:** Managed Security Services Provide;
- **PaaS:** Platform as a Service;
- **SaaS:** Software as a Service;
- **SAL:** Stato Avanzamento Lavoro/i;
- **SOC**: Security Operation Center.

3 DEFINIZIONE DEI SERVIZI OGGETTO DELLA FORNITURA

3.1 Oggetto della Fornitura

L'oggetto della Fornitura è rappresentato dal complesso dei servizi di Security Consulting descritti nel Capitolo 4 del presente Capitolato tecnico e dalle attività ad essi associate volte a garantire la sicurezza delle infrastrutture e dei dati dell'Amministrazione, a rispondere in maniera efficace in caso di attacchi informatici, a mantenere la perfetta efficienza delle infrastrutture di sicurezza ICT nonché a fornire, alla Committente e/o all'Amministrazione, il supporto necessario per assicurare il costante allineamento con l'evoluzione tecnologica del mercato ICT security e a definirne la crescita, in coerenza con gli obiettivi strategici dell'Amministrazione stessa, secondo la seguente articolazione:

Security Consulting Services	
Servizi On Demand	**Servizi Continuativi**
- Security Strategy Consulting;	- Incident Response Team.
- Security Risk Management;	
- Compliance Consulting;	
- Enforcement Policy e Linee Guida;	
- Security Engineering;	
- Security Assessment;	
- Security Audit.	

Per l'erogazione dei servizi oggetto del presente Capitolato tecnico, l'Impresa dovrà definire le seguenti figure professionali, il cui ruolo potrà comunque essere assunto anche dalla medesima persona:

- **Responsabile del contratto**, il quale ha la responsabilità di gestire e risolvere tutte le problematiche legate al corretto svolgimento del contratto (es. fatturazione, verifica del rispetto dei livelli di servizio, definizione e aggiornamento del team di cui al paragrafo 4.5); nonché la richiesta di attivazione di nuovi Servizi, tra quelli definiti;
- **Responsabile tecnico** per l'erogazione dei servizi, avente la responsabilità di coordinare dal punto di vista operativo tutte le attività legate ai servizi oggetto del presente Capitolato tecnico e di essere il punto di riferimento tecnico per la gestione dei Servizi, tra quelli definiti. Il Responsabile tecnico dovrà inoltre coordinare tutte le attività e produrre resoconti periodici, da presentare per discussione durante i SAL di progetto.

I SAL, da tenere con cadenza mensile e/o su esplicita richiesta del Committente/ Amministrazione, dovranno riguardare almeno i seguenti argomenti:

- dettaglio delle attività svolte e di quelle ancora da svolgere;
- eventuali problematiche insorte;
- questioni aperte di carattere strategico/metodologico da sottoporre all'attenzione del/la Committente/Amministrazione.

A fronte di eventuali problematiche che dovessero presentarsi, il SAL dovrà comprendere anche le relative proposte di risoluzione e la relativa ripianificazione delle attività impattate.
Il Responsabile tecnico del servizio, durante i SAL mensili, dovrà presentare alla Committente il "**Resoconto Attività**", contenente, tra l'altro, lo stato della/e fase/i in lavorazione e i giorni persona effettivamente impiegati nell'erogazione del/i servizio/i. Tali informazioni e dati saranno successivamente vagliati dalla Committente in sede di verifica di conformità.
L'Impresa, al momento della stipula, dovrà comunicare al Committente/Amministrazione il numero di recapito telefonico e l'indirizzo e-mail attraverso i quali contattare le suddette figure professionali.
Per le attività svolte dalle figure di Responsabile del contratto e di Responsabile tecnico, non sarà riconosciuto alcun effort e pertanto nessun corrispettivo economico, ritenendosi gli stessi ricompresi nell'offerta economica presentata.

3.2 Sedi dell'Amministrazione e della Committente

Le prestazioni oggetto del presente Capitolato dovranno essere erogate, a seconda delle esigenze specifiche di progetto, presso:

- le sedi di Roma della CdC, ovvero via Antonio Baiamonti, n. 25, nonché presso le altre sedi della stessa che verranno eventualmente indicate in sede di esecuzione;
- la sede della Committente, ovvero via Mario Carucci, n.99, Roma;
- la sede dell'Impresa.

Eccezionalmente, su richiesta della Committente/Amministrazione, le prestazioni potranno essere erogate presso sedi di Amministrazioni che utilizzano i servizi IT della CdC, quali ad esempio Avvocatura dello Stato, CNEL, ect.

3.3 Durata del contratto

La durata massima del contratto è fissata in 36 mesi decorrenti dalla Data di Attivazione di cui al par. 5.4 del presente Capitolato.

4 DESCRIZIONE DELLA FORNITURA

4.1 Security Consulting

Di seguito è fornita una descrizione di massima del contesto tecnologico e delle caratteristiche tecniche dei servizi richiesti, relativi al Security Consulting, che saranno organizzati in due aree principali:

- **Servizi On Demand**: ossia tutti i servizi consulenziali ad alto valore aggiunto che saranno definiti a fronte di una richiesta specifica dalla Committente e/o dall'Amministrazione e valutati e consuntivati in funzione dei deliverable e delle tempistiche di esecuzione concordate;
- **Servizi Continuativi**: ossia tutti i servizi che richiedono una continuità operativa presso le sedi operative della Amministrazione e/o Committente, al fine di offrire un servizio di presidio e/o di consulenza dedicato a specifici ambiti della sicurezza.

Il Fornitore prende atto che, nel corso dell'erogazione dei servizi, a fronte delle evoluzioni in ambito ICT, l'introduzione di nuove tecnologie potrà comportare significative variazioni del contesto tecnologico di inizio Fornitura e si impegna ad erogare i servizi richiesti adeguando le conoscenze del personale impiegato nell'erogazione degli stessi o inserendo nei gruppi di lavoro risorse con adeguati skill, senza alcun onere aggiuntivo per la Committente e/o l'Amministrazione.

Tutti gli eventuali strumenti utilizzati a supporto dell'erogazione dei servizi descritti nel presente Capitolato saranno a totale onere dell'Impresa.

4.2 Servizi On Demand

Nell'ambito dell'insieme di attività che definiscono il servizio di Security Consulting, è prevista l'attivazione su richiesta dei Servizi On Demand, relativamente alle **aree di intervento** che saranno di seguito illustrate.

4.2.1 Security Strategy Consulting

Attività mirata a supportare l'Amministrazione nella definizione delle scelte strategiche inerenti il governo della Sicurezza delle informazioni, degli indirizzi organizzativi e tecnologici in materia di IT Security e dell'approccio gestionale da adottare a fronte di nuovi paradigmi architetturali, scenari di attacco e situazioni di rischio consolidate.

In particolare il servizio sarà orientato a supportare l'Amministrazione sui seguenti ambiti:

- definizione, consolidamento e manutenzione delle tassonomie e delle classificazioni in materia di sicurezza informatica (es. tassonomia e classificazione incidenti, classificazione degli asset, ecc.);
- definizione degli elementi di base inerenti il processo di gestione della sicurezza delle informazioni (definizione del rischio accettabile, identificazione delle minacce e degli elementi di applicabilità ai contesti di riferimento, ecc.);
- identificazione delle iniziative in materia di sicurezza informatica e sicurezza delle informazioni in funzione dell'introduzione di nuovi elementi infrastrutturali, organizzativi o applicativi all'interno del contesto di riferimento;

- valutazione degli impatti e dei rischi inerenti i contratti di servizio dell'Amministrazione, relativi a problematiche di sicurezza intrinseca;
- indirizzo delle eventuali iniziative in materia di sicurezza informatica e sicurezza delle informazioni, in funzione delle "lesson learned" derivanti dalla gestione di incidenti di sicurezza, risultati di audit interni (o di terza parte), security assessment periodici;
- valutazione degli impatti organizzativi e tecnici a fronte dei benefici sugli elementi di mitigazione offerti relativamente all'introduzione di nuovi paradigmi, processi o soluzioni orientate all'enforcement della sicurezza delle informazioni e all'IT Security;
- gestione dei processi di escalation e di comunicazione con l'esterno in caso di incidenti di sicurezza con rilevanza penale.

Il servizio sarà erogato in modalità progettuale secondo le indicazioni riportate nel paragrafo 5.3 .

4.2.2 **Security Risk Management**

Attività relativa al supporto specialistico per la definizione e adeguamento della metodologia di analisi del rischio generale e specifico per i contesti operativi di riferimento, inteso come insieme di policy, procedure, standard, check list e istruzioni operative in grado di governare il processo di analisi e gestione del rischio, e l'esecuzione delle campagne di analisi e gestione del rischio su processi e infrastrutture, in accordo con il modello definito.

Il servizio specifico si articola nelle seguenti sotto-attività:

- supporto consulenziale per la definizione o l'adeguamento dei processi di analisi e gestione del rischio in termini di modelli di calcolo e mitigazione del rischio, identificazione e mantenimento delle contromisure applicabili e del loro apporto in fase di mitigazione, consulenza nella definizione del modello di valutazione del rischio, governo e accettazione dello stesso in funzione del processo generale di governo della sicurezza. Tale attività dovrà essere contestualizzata anche in funzione dei paradigmi di deployment adottati dall'Amministrazione (On-premise, Cloud oriented in modalità IaaS/PaaS/SaaS, MSSP, ecc.) e delle specificità inerenti le contromisure applicabili sul paradigma specifico (es. Azure, AWS, ecc.);
- gestione delle attività di analisi del rischio in funzione della metodologia definita, contestualizzandola allo scenario di deployment dello specifico processo/infrastruttura;
- gestione delle attività di mitigazione del rischio sempre in funzione della metodologia definita, basandosi sui controlli applicabili al contesto di riferimento stabiliti in fase di definizione iniziale della metodologia, e riportando all'Amministrazione l'approccio seguito e il livello di mitigazione del rischio raggiungibile;
- supporto all'Amministrazione nel processo decisionale di accettazione o riesame del piano di gestione del rischio definito nelle fasi di analisi e gestione;
- supporto all'Amministrazione nel definire l'esposizione derivante dall'adozione di nuovi servizi, nuove tecnologie o modifiche infrastrutturali in funzione dei vincoli

presenti, delle best practices di gestione delle sicurezza e dei rischi intrinsechi derivanti dall'adozione stessa;

- individuare e mantenere le contromisure adottabili al fine di permettere all'Amministrazione la strategia più efficace da adottare per ridurre il rischio.

Il servizio sarà erogato in modalità progettuale secondo le indicazioni riportate nel paragrafo 5.3 .

4.2.3 **Compliance Consulting**

Tale servizio è orientato a redigere e/o aggiornare la documentazione relativa al sistema privacy secondo le indicazioni contenute nel documento pubblicato sul sito di AgID (www.agid.gov.it), dal titolo "*Misure minime per la sicurezza ICT delle pubbliche amministrazioni*", come aggiornato e/o modificato alla data di esecuzione del contratto, nonché a valutare e adeguare i sistemi e le politiche di sicurezza aziendali rispetto alle leggi e ai regolamenti vigenti.

In particolare è richiesto il supporto necessario all'Amministrazione per indirizzare eventuali iniziative, in particolare contestualizzando i provvedimenti e le prescrizioni applicabili al dominio della Corte dei conti con i seguenti obiettivi:

- individuare gli ambiti di impatto dell'eventuale prescrizione;
- identificare il differenziale tra l'esistente e quanto specificato all'interno della prescrizione di riferimento, massimizzando l'uso di quanto già in essere;
- definire un piano di adeguamento che includa sia gli interventi in ambito organizzativo, sia in ambito tecnico;
- validare i piani di rientro proposti dalle varie realtà interne con il supporto delle strutture tecniche e dei servizi di consulenza previsti all'interno della presente Gara.

Il servizio sarà orientato anche all'identificazione delle prescrizioni della normativa vigente e alla loro valutazione così come descritto in precedenza, oltre al monitoraggio di eventuali iniziative al fine di supportare l'organizzazione per un adeguamento sostenibile del contesto.

Dovrà essere previsto per tutto il periodo di riferimento un supporto sia per l'implementazione del modello di valutazione privacy in accordo con le politiche interne, sia il coordinamento del processo di valutazione, analisi e redazione della documentazione necessaria a supporto.

Il servizio sarà erogato in modalità progettuale secondo le indicazioni riportate nel paragrafo 5.3 .

4.2.4 **Enforcement Policy e Linee Guida**

Nell'ambito del presente servizio è prevista l'attività di redazione di nuove politiche e linee guida di sicurezza, laddove l'Amministrazione ne riscontri la mancanza, o di adeguamento delle politiche e procedure esistenti, rispetto ai cambiamenti infrastrutturali e organizzativi.

Il servizio dovrà prevedere una o più attività di gap analysis orientate a verificare e validare lo stato delle normative esistenti, il loro grado di efficacia e rispondenza rispetto agli obiettivi di business, e predisporre un piano di applicazione orientato al miglioramento continuo e alla copertura di eventuali problematiche o ambiti non ancora indirizzati.

Il servizio sarà erogato in modalità progettuale secondo le indicazioni riportate nel paragrafo 5.3 .

4.2.5 **Security Engineering**

Il servizio è orientato a identificare, ingegnerizzare e integrare le soluzioni di sicurezza in uso o da introdurre all'interno del contesto della Corte dei conti in funzione delle minacce esistenti, affinché siano coerenti con le strategie aziendali.

In particolare il servizio risulta orientato ai seguenti ambiti:

- prendere in consegna le architetture di sicurezza in essere e supportare l'Amministrazione nel definire il piano di enforcement tecnico in funzione di quanto già acquisito o di eventuali best practices consolidate;
- supportare il processo di analisi dei requisiti iniziali e la definizione delle configurazioni di sicurezza più idonee, nell'ambito della realizzazione di nuovi servizi o eventuali change sui servizi esistenti;
- redigere i progetti di architettura generale, i progetti esecutivi e i manuali operativi relativi alle soluzioni di sicurezza, normalizzando la documentazione mancante di quanto già acquisito e successivamente manutenendo o integrando la documentazione in funzione dei change previsti nel contesto di riferimento;
- gestire/supportare eventuali attività di benchmarking sui servizi e sulle tecnologie specifiche, sfruttando sia gli ambienti di collaudo della Corte dei conti (sia eventuali laboratori ad-hoc) in funzione delle soluzioni o servizi da valutare;
- supportare la contestualizzazione tecnica dei piani di rientro o del processo di gestione del rischio identificando le soluzioni tecniche o le integrazioni sul contesto IT che possano indirizzare e mitigare in maniera corretta ed efficace il controllo richiesto;
- definire soluzioni e best practices per l'innalzamento della sicurezza applicativa e dei dati da esse gestiti, durante tutto il ciclo di vita dell'applicazione stessa;
- identificare le sorgenti necessarie e progettare le eventuali regole di correlazione per l'identificazione degli use case definiti in fase di definizione degli scenari di rischio o applicazione delle lesson learned in fase di incident response;
- identificare i modelli di integrazione più efficaci ed efficienti tra sistemi, strumenti di sicurezza e applicazioni per l'implementazione di specifici controlli di sicurezza;
- supportare operativamente i processi di change nelle fasi di SAL e la programmazione delle attività, in accordo con le strutture di Ingegneria, Conduzione e Security Operation, per tutte le attività inerenti architetture e configurazioni relative alla sicurezza.

Il servizio sarà erogato in modalità progettuale secondo le indicazioni riportate nel paragrafo 5.3 .

4.2.6 **Security Assessment**

Il servizio è orientato alla validazione sul campo delle misure di sicurezza implementate a livello logico in relazione al livello di rischio nei confronti di diversi agenti di minaccia e di diversi ambiti di applicazione, analizzando sia la resistenza agli attacchi dei sistemi esposti pubblicamente e delle difese perimetrali nel loro complesso, che il livello di sicurezza dei sistemi sulle reti private e dell'infrastruttura di networking locale e geografica.

In particolare si vuole verificare, in relazione allo stato attuale della tecnologia ed alle metodologie di attacco pubblicamente conosciute, la possibilità di sfruttare eventuali vulnerabilità sui servizi e sulle applicazioni installate, e la robustezza delle configurazioni in essere al fine di accedere illegalmente, rubare o manomettere informazioni, commettere atti di vandalismo, interrompere i servizi erogati.

Si evidenzia che i risultati dell'analisi dovranno essere improntati più ad un punto di vista tecnico-operativo che ad un'analisi teorico-procedurale in quanto serviranno come base per valutare il livello di sicurezza reale e gli investimenti effettuati e pianificare i nuovi interventi in ottica di sicurezza informatica e protezione dei dati e del patrimonio aziendale.

I test potrebbero essere eseguiti su sistemi e reti in esercizio, per cui tutte le attività che potrebbero causare blocchi o disservizi dovranno essere preventivamente concordate e pianificate e potranno tenersi nell'orario indicato al successivo par. 4.4 relativamente ai servizi on demand.

Il team che effettuerà le analisi dovrà tenere traccia scritta delle attività svolte, comprensiva di data e ora di inizio/fine e sistemi/reti coinvolti; dovrà altresì monitorare il corretto funzionamento di alcuni servizi e sistemi critici preventivamente concordati ed interrompere le attività ed allertare i referenti dell'Amministrazione/Committente in caso di disservizi.

Nell'ambito dei servizi di Security Assessment si riporta una lista, non esaustiva, delle tipologie di test che potrebbero essere richieste dall'Amministrazione:

- *Vulnerability Assessment infrastrutturale*: analisi dinamica su uno specifico ambito finalizzata a rilevare lo stato intrinseco della sicurezza dei servizi esposti in termini di vulnerabilità sui sistemi e sui servizi stessi e configurazioni insicure presenti;
- *Penetration Test infrastrutturale e applicativo*: analisi dinamica su uno specifico ambito o applicazione finalizzato ad identificare le vulnerabilità applicative e di sistema e validarne il reale grado di utilizzo simulando un eventuale scenario di attacco e verificando le catene di vulnerabilità utilizzabili e il loro effettivo impatto sui dati e sui servizi;
- *Wireless Penetration Test*: analisi dinamica e analisi della configurazione di eventuali reti wireless e validazione delle vulnerabilità sia sui sistemi di accoglienza, che sui sistemi di rete specifici, identificando gli scenari di attacco applicabili al contesto di riferimento;
- *Mobile Application Penetration Test*: analisi dinamica di una specifica App mobile e del suo back-end finalizzato a identificare le vulnerabilità applicative e di sistema e validarne il reale grado di utilizzo simulando un eventuale scenario di attacco e

verificando le catene di vulnerabilità utilizzabili e il loro effettivo impatto sui dati e sui servizi;

- *Source Code Auditing*: servizio di analisi statica del codice finalizzato alla verifica integrale della sicurezza di un'applicazione (già durante il progetto di sviluppo). Tale attività dovrà basarsi sull'analisi dei flussi di input seguendo la logica delle diverse componenti applicative, validando l'effettiva raggiungibilità di determinate funzioni vulnerabili o errori di configurazione o utilizzo di specifici framework e sistemi. Il servizio dovrà coprire i linguaggi Java e .NET, XML, CSS, HTML5 nonché i framework MVC in uso nel contesto di riferimento come Hibernate, Spring, Struts, etc.;
- *Configuration Audit*: Servizio di analisi statica delle configurazioni dei sistemi a perimetro, finalizzata a valutare eventuali problematiche legate a mis-configurazioni o agli aggiornamenti dei sistemi in uso e alla compliance delle configurazioni rispetto alle linee guida di hardening o agli standard definiti dall'Amministrazione o dei requisiti di compliance richiesti;
- *Cloud Security Auditing*: analisi statica e dinamica dei servizi esposti in ambito Cloud, sia in termini della configurazione dei servizi infrastrutturali del tier dedicato all'Amministrazione (modello di segregazione, esposizione dei servizi, utenti abilitati e livelli di privilegio concessi), sia delle applicazioni esposte con le stesse modalità illustrate in precedenza.

Al termine delle attività svolte nell'ambito del servizio appena descritto, dovranno essere realizzati due rapporti:

- un **Executive Summary**, destinato prevalentemente al management ed al personale non tecnico per una comprensione immediata del problema e della sua distribuzione in termini dipartimentali;
- un **Technical Report**, con tutte le indicazioni necessarie per la comprensione del problema, per la sua classificazione in termini di priorità e per l'identificazione delle strutture aziendali più idonee alla risoluzione.

4.2.6.1 EXECUTIVE SUMMARY

L'Executive Summary dovrà illustrare i principali rischi a cui l'azienda è sottoposta a causa delle vulnerabilità riscontrate e dovrà fornire un messaggio incisivo allo scopo di provocare un adeguato livello di reazione da parte del management stesso. Nel documento dovranno essere concentrati e riassunti i risultati esposti nel report tecnico, conservandone la sequenza e la struttura concettuale.

L'Executive Summary dovrà inoltre includere un piano di azione ad alto livello per illustrare, su specifiche classi di priorità (Breve, Medio e Lungo Termine), le macro-categorie di problemi rilevati sui sistemi oggetto dell'analisi e scandire un opportuno piano di rientro.

4.2.6.2 TECHNICAL REPORT

Il Technical Report dovrà essere articolato in modo da mantenere una separazione logica tra le differenti piattaforme soggette ad analisi.

Per ogni piattaforma in esame, oltre a fornire una precisa segnalazione delle varie vulnerabilità riscontrate e/o punti deboli del sistema (in termini di porte, servizi e informazioni del sistema, o circa eventuali analisi condotte in ambito locale) dovranno essere riportate anche indicazioni precise sulle possibili soluzioni (in termini di patch, di configurazioni necessarie e suggerimenti migliorativi) al fine di mitigare i potenziali rischi generati dal loro sfruttamento.

Ogni problematica riportata dovrà essere descritta in una sezione specifica di approfondimento tecnico. Tale sezione descrittiva dovrà essere composta almeno da:

- descrizione di dettaglio della problematica rilevata;
- riferimenti a documentazione pubblica per ulteriori approfondimenti tecnici;
- suggerimenti provvisori realizzati dal team di analisi;
- workaround possibili, qualora applicabili;
- soluzioni perimetrali di protezione, qualora applicabili.

Per ogni vulnerabilità tecnica dovrà essere effettuata un'analisi "tecnica" del rischio (basata sullo standard CVSS:Common Vulnerability Scoring System) che prende in considerazione popolarità e semplicità dell'attacco commisurata al valore del sistema e al grado di compromissione raggiunto.

Il servizio sarà erogato in modalità progettuale secondo le indicazioni riportate nel paragrafo 5.3 .

4.2.7 **Security Audit**

Nell'ambito del presente servizio è prevista la gestione delle campagne di audit di conformità rispetto alle normative vigenti o agli standard interni definiti per lo specifico ambito sotto analisi.

Le attività da svolgere sono le seguenti:

- analisi delle attività degli Amministratori di Sistema, in conformità al Provvedimento del Garante per la Privacy;
- valutazione dell'effettiva attuazione delle policy, delle linee guida e degli standard di sicurezza definiti dalla Funzione Sicurezza;
- verifica della conformità delle configurazioni in esercizio alle normative, alle best practices e agli standard di riferimento;
- validazione della rispondenza dei contratti in essere rispetto ai vincoli delle normative vigenti applicabili, soprattutto per i servizi Cloud Oriented;
- valutazione del grado di awareness del personale interno rispetto a specifiche problematiche di sicurezza o al recepimento di determinate normative interne;
- rilevazione dello stato attuale della Gestione della Sicurezza delle informazioni rispetto agli standard ISO/IEC 27001 e alle linee guida ISO inerenti la gestione del rischio e i controlli di sicurezza, al fine di supportare future attività progettuali che prevedono una corretta definizione degli obiettivi strategici ed una puntuale individuazione degli interventi di miglioramento.

Il servizio sarà erogato in modalità progettuale secondo le indicazioni riportate nel paragrafo 5.3 .

4.3 **Servizi Continuativi**

I servizi continuativi sono costituiti da interventi specifici che, per loro natura, hanno la caratteristica di essere continuativi nel tempo e mirati alla gestione giornaliera di specifici task direttamente presso le sedi dall'Amministrazione e/o Committente.

I suddetti servizi saranno attivati secondo le modalità indicate nel successivo par. 5.4 .

4.3.1 **Incident Response Team**

L'unico Servizio continuativo richiesto nella presente procedura di gara è costituito dal servizio di Incident Response Team. Si tratta di uno dei servizi più critici nel contesto della Corte dei conti in quanto atto a garantire e supportare l'Amministrazione/Committente, del rispetto e nella corretta esecuzione di tutti i processi di gestione degli incidenti di sicurezza ed escalation.

Il servizio prevede un'attività operativa a supporto per l'analisi approfondita di eventuali use case categorizzati, come incidenti di sicurezza. A fronte di un incidente di sicurezza l'Incident Response Team si occuperà della definizione del livello di impatto, delle entità da coinvolgere e della contromisure da adottare.

Inoltre l'Incident Response Team, dovrà svolgere un'attività consulenziale di supporto ai processi e all'enforcement tecnologico in funzione delle lesson learned acquisite durante le analisi svolte.

I servizi operativi di analisi in particolare riguardano le seguenti attività:

- coordinamento delle attività di Incident Response relativamente a problematiche di sicurezza;
- supporto nell'acquisizione corretta delle evidenze dei case analizzati;
- servizio di Log o Event Analysis;
- Malware Forensic;
- Network & System Forensic;
- supporto ai processi di escalation verso le entità interne e esterne (inclusi organi di Polizia Giudiziaria).

I servizi consulenziali riguarderanno invece:

- supporto alla incident management strategy, ossia definizione delle azioni di contenimento, modalità di gestione del rapporto con le entità interne ed esterne, ecc.;
- gestione delle iniziative di Enforcement sui processi di sicurezza in funzione delle lesson learned rilevate in fase di analisi;
- gestione dell'ingegneria del monitoraggio, in termini di definizione degli use case relativi negli incidenti di sicurezza, progettazione delle regole di correlazione e validazione dei sistemi di rilevazione in essere;
- supporto ai processi di tuning dei sistemi di rilevazione degli allarmi di sicurezza in collaborazione con i Servizi On Demand di Security Engineering.

Si precisa che a fronte di gravi incidenti di sicurezza, dovranno essere erogati interventi on site presso le sedi indicate al paragrafo 3.2, stimati per un massimo di circa 2 interventi per ciascun anno; per tali interventi non sarà dovuto alcun corrispettivo ulteriore.

4.4 Orario di servizio

L'orario dei servizi di Security Consulting è riportato nel seguito:

a) i Servizi On Demand sono svolti nei giorni feriali dal lunedì al venerdì, indicativamente tra le 09.00 e le 18.00, fatte salve eventuali eccezioni concordate in anticipo con il Fornitore per permettere lo svolgimento degli stessi anche in fasce orarie/giorni differenti;
b) i Servizi Continuativi, sono svolti nei giorni feriali dal lunedì al venerdì indicativamente dalle 09.00 alle 18.00.

A fronte di gravi incidenti di sicurezza si richiede che il personale costituente il servizio continuativo di Incident Response Team, di cui al paragrafo 4.3.1 fornisca:

- disponibilità agli interventi di cui al precedente punto b) garantita anche per l'intera giornata (24 ore) dei giorni feriali, ed anche per l'intera giornata (24 ore) del sabato e/o della domenica e/o dei festivi, anche on site.

In aggiunta ai punti a) e b) sopra riportati, eventuali estensioni dell'orario di servizio saranno richieste dalla Committente e/o dall'Amministrazione con il seguente preavviso minimo:

- nella stessa giornata lavorativa: 1 ora;
- disponibilità dei servizi il sabato, la domenica e/o nei giorni festivi: 4 ore.

L'estensione dell'orario di servizio è richiesta via posta elettronica e, se pervenuta nel periodo di preavviso prestabilito, non è soggetta all'accettazione da parte del Fornitore.

Si precisa che per giorni festivi devono intendersi le festività a carattere nazionale nonché, per i servizi erogati presso la sede centrale dell'Amministrazione, il 29 giugno.

4.5 Gruppo di lavoro e Profili professionali richiesti

L'Impresa, per formare il team che si occuperà delle attività previste per il *Security Consulting Services*, dovrà avvalersi di personale specializzato nelle varie aree d'intervento descritte al precedente paragrafo 4.1 e in possesso di competenze specifiche nonché di certificazioni funzionali al ruolo di riferimento.

In particolare è prevista la presentazione di un team di lavoro, i cui profili dovranno soddisfare quelli riportati nei successivi paragrafi 4.5.1, 4.5.2, 4.5.3, 4.5.4, 4.5.5, 4.5.6, 4.5.7 e 4.5.8, che il Fornitore dovrà impiegare nelle varie aree di intervento, definendo esplicitamente la percentuale di impiego che dovrà essere riportata nel modello organizzativo di riferimento.

In Tabella 1 si riporta la stima di impegno in GP previsto per l'esecuzione delle attività all'interno del perimetro dei Servizi On Demand, mentre in Tabella 2 si riporta il mix di impegno delle Figure Professionali richieste, sul medesimo perimetro di Servizi.

Servizi On Demand	Totale GP per servizio
Security Strategy Consulting	100
Security Risk Management	350
Compliance Consulting	350
Enforcement Policy e Linee Guida	400
Security Engineering	600
Security Assessment	200
Security Audit	300
Totale	**2300**

Tabella 1 – Stima impegno previsto per servizio

Figura Professionale	Servizi On Demand						
	Security Strategy Consulting	Security Risk Management	Compliance Consulting	Enforcement Policy e Linee Guida	Security Engineering	Security Assessment	Security Audit
Security Principal	**30%**	**8%**	**4%**	**4%**	**8%**	**10%**	**12%**
Security Solution Architect	*	**0%**	**0%**	**0%**	**60%**	**0%**	**0%**
Senior Information Security Consultant	*	**32%**	**36%**	**36%**	**0%**	**0%**	**0%**
Junior Information Security Consultant	**0%**	**60%**	**60%**	**60%**	**32%**	**0%**	**40%**
Senior Security Pentester	**0%**	**0%**	**0%**	**0%**	**0%**	**70%**	**0%**
Senior Security Auditor	*	**0%**	**0%**	**0%**	**0%**	**20%**	**48%**

*a seconda della tematica in oggetto, verrà ripartito il restante 70% di effort sulle relative figure di riferimento. Per il dimensionamento a base d'Asta è stata considerata una suddivisione equamente distribuita dell'effort, pari al 23,33% per le figure professionali indicate.

Tabella 2 - Mix di impegno per figura professionale e Servizio

In Tabella 3 si riporta la stima di impegno in GP previsto per l'esecuzione delle attività all'interno dei Servizi Continuativi, mentre in Tabella 4 si riporta il mix di impegno delle Figure Professionali richieste, sul medesimo perimetro di servizi.

Servizi Continuativi	Totale GP servizio
Incident Responce Team	1320
Totale	**1320**

Tabella 3 - Stima impegno previsto per il Servizio IRT

Figura Professionale	Servizi Continuativi
	Incident Response Team
Senior Security Analyst	50%
Junior Security Analyst	50%

Tabella 4 - Mix di impegno per figura professionale e Servizio

I mix di impegno riportati nelle tabelle precedenti, sono quelli ritenuti ottimali dalla Committente/Amministrazione; tuttavia il fornitore in fase di esecuzione può proporre di variarne la composizione sia pur in misura contenuta e coerente con le percentuali di impiego generalmente utilizzate per risorse di servizi analoghi, per modulare i gruppi di lavoro secondo la propria usuale organizzazione lavorativa, garantendo comunque la qualità del servizio prestato, previa accettazione del mix proposto dalla Committente/Amministrazione, prima della accettazione formale della Proposta Tecnica Economica (PTE) per i Servizi On Demand e dell'attivazione del servizio di Incident Response Team per i Servizi Continuativi (quest'ultima come prevista nel successivo par. 5.4).

***

Le qualifiche richieste nella documentazione di gara devono essere state rilasciate da un ente certificatore o da un'impresa di formazione accreditata da Accredia o un altro organismo da essa riconosciuto attraverso i cosiddetti multi-lateral agreement.

Le risorse in possesso delle certificazioni specificate e/o richieste e/o offerte dall'Impresa, dovranno essere rese disponibili per l'intera efficacia del contratto e dovranno essere impiegate nei team di lavoro che garantiscono l'erogazione dei servizi oggetto della fornitura anche senza espressa richiesta dell'Amministrazione.

Nei successivi paragrafi vengono descritti i requisiti minimi e le certificazioni obbligatorie richieste per ogni Figura professionale.

4.5.1 **Security Principal**

Profilo

Laureato con laurea specialistica in materie scientifiche, con anzianità lavorativa maggiore di 12 (dodici) anni, da computarsi successivamente alla data di conseguimento della laurea, di cui almeno 5 (cinque) anni di provata esperienza nella specifica funzione.

È richiesta, inoltre, in relazione alla tipologia di attività su cui verrà impiegata la risorsa:

- conoscenza della metodologia di Project Management;
- esperienza di Project Management in progetti analoghi;
- conoscenza approfondita dei processi di Security Governance e Security Management;

- conoscenza approfondita delle metodologie di vulnerability assessment, penetration test, compliance management e security audit;
- esperienza nel disegno e nella valutazione dei sistemi per la gestione della sicurezza delle informazioni;
- conoscenza delle metodologie e degli strumenti operativi richiesti in progetti di IT Security;
- conoscenza dei processi e delle procedure operative IT;
- conoscenza delle tecnologie principali per la sicurezza IT;
- certificazione CISM (Certified Information Security Manager) in possesso da almeno tre anni al momento di presentazione dell'offerta.

4.5.2 **Security Solution Architect**

Profilo

Laureato in discipline scientifiche con anzianità lavorativa di almeno 8 (otto) anni, da computarsi successivamente alla data di conseguimento del diploma di laurea, di cui almeno 4 (quattro) anni di provata esperienza nella specifica funzione.

È richiesta, inoltre, in relazione alla tipologia di attività su cui verrà impiegata la risorsa:

- capacità di comprendere l'infrastruttura sotto analisi e le relazioni tra i differenti sistemi e componenti infrastrutturali;
- esperienza nell'analisi e nella valutazione delle configurazioni e delle regole tecniche delle principali soluzioni di sicurezza utilizzate per proteggere l'infrastruttura e i servizi (Firewall, IPS/IDS, SIEM, soluzioni anti-malware, Web Application Firewall, Database Monitoring, servizi Anti-DDoS, servizi cloud oriented per la sicurezza, ecc.);
- esperienza nell'analisi di un'infrastruttura IT complessa volta all'individuazione di problematiche architetturali che ne potrebbero compromettere la sicurezza;
- esperienza nella verifica dell'efficacia delle misure tecniche ed organizzative preposte alla sicurezza di un'infrastruttura IT complessa;
- consolidata esperienza nella progettazione della sicurezza ICT maturata in contesti analoghi;
- conoscenza approfondita delle problematiche di sicurezza delle infrastrutture IT;
- conoscenza delle metodologie e degli strumenti operativi richiesti per verificare l'efficacia delle contromisure di sicurezza poste a salvaguardia delle infrastrutture IT;
- esperienza nell'identificazione di soluzioni tecnologiche ed organizzative da porre in essere per ottimizzare e migliorare le configurazioni e le politiche e per traguardare la piena adozione delle contromisure previste;
- conoscenza delle tecnologie principali per la sicurezza IT, soprattutto in ambito sicurezza cloud, sicurezza minacce di nuova generazione, modalità di contenimento, ecc.;

- ottima conoscenza sistemi di correlazione eventi, progettazione regole di correlazione e tuning sistemi di analisi eventi con esperienza di integrazione in contesti analoghi;
- buona conoscenza sistemi di autenticazione, specialmente sistemi di Identity & Access Management con esperienza di integrazione su ambienti analoghi;
- conoscenza delle tecnologie in uso nel contesto di riferimento, con esperienza nella configurazione e nell'inserimento in rete delle stesse, in funzione delle minacce riscontrate.

4.5.3 **Senior Information Security Consultant**

Profilo

Laureato in discipline scientifiche con anzianità lavorativa di almeno 8 (otto) anni, da computarsi successivamente alla data di conseguimento del diploma di laurea, di cui almeno 4 (quattro) anni di esperienza nella specifica funzione.

È richiesta, inoltre, in relazione alla tipologia di attività su cui verrà impiegata la risorsa:

- capacità di coordinamento dei Consulenti Junior;
- conoscenza dei processi e delle procedure operative IT;
- conoscenza dei sistemi di controllo in ambito IT;
- conoscenza complessiva delle problematiche di sicurezza dei dati e delle informazioni;
- conoscenza delle metodologie e delle linee guida ISO in materia di Risk Assessment e Risk Treatment, e degli strumenti a supporto per le due fasi del processo di gestione del rischio;
- conoscenza delle linee guida ISO sui controlli di sicurezza in ambito enterprise e cloud ed esperienza nella contestualizzazione nel processo di mitigazione del rischio;
- esperienza consolidata nella realizzazione di sistemi SGSI in accordo con la norma ISO:27001;
- esperienza consolidata nella conduzione di Risk Assessment;
- esperienza consolidata nella definizione di modelli per l'analisi del rischio applicabili a paradigmi infrastrutturali e organizzativi specifici;
- conoscenza approfondita della normativa sulla Privacy e dei Provvedimenti del Garante, sia in ambito Italiano che Europeo;
- conoscenza approfondita delle direttive dell'AgID in materia di sicurezza delle informazioni e continuità operativa dei servizi;
- esperienza consolidata nella valutazione di analisi di compliance in materia Privacy e direttive AgID su contesti analoghi, e nella definizione e governo dei piani di rientro;
- esperienza consolidata nella redazione della documentazione a supporto per i processi di compliance rispetto alle normative applicabili (es. Documento Programmatico della Sicurezza, Studio di fattibilità per la continuità operativa del CAD, ecc.);

- esperienza consolidata nella redazione di policy e linee guida di sicurezza a supporto dei processi organizzativi su diversi ambiti di applicazione (es. classificazione delle informazioni, gestione del rischio, gestione degli incidenti, identificazione degli utenti, utilizzo sicuro dei servizi informatici, ecc.)
- **qualifica di Lead Auditor ISO 27001 aggiornata all'ultima release del 2013**.

4.5.4 **Junior Information Security Consultant**

Profilo

Laureato con diploma di laurea in discipline scientifiche con anzianità lavorativa di almeno 2 (due) anni, da computarsi successivamente alla data di conseguimento del diploma di laurea, di cui almeno un anno di esperienza nella specifica funzione.

È richiesta, inoltre, in relazione alla tipologia di attività su cui verrà impiegata la risorsa:

- conoscenza delle tecniche e delle metodologie di Risk Management;
- partecipazione in progetti di Risk Assessment;
- partecipazione alla definizione di modelli per l'analisi del rischio applicabili a paradigmi infrastrutturali e organizzativi specifici;
- conoscenza della normativa sulla Privacy e dei Provvedimenti del Garante;
- partecipazione nella redazione della documentazione a supporto per i processi di compliance rispetto alle normative applicabili (es. Documento Programmatico della Sicurezza, Studio di fattibilità per la continuità operativa del CAD);
- partecipazione nella redazione di policy e linee guida di sicurezza a supporto dei processi organizzativi;
- esperienza nella conduzione di IT Audit.

4.5.5 **Senior Security Pentester**

Profilo

Laureato in discipline scientifiche con anzianità lavorativa di almeno 6 (sei) anni, da computarsi successivamente alla data di conseguimento del diploma di laurea.

È richiesta, inoltre, in relazione alla tipologia di attività su cui verrà impiegata la risorsa:

- esperienza di almeno 6 (sei) anni in una o più delle seguenti aree di attività:
  - analisi dinamica delle vulnerabilità e penetration testing sia in ambito applicativo che sulle infrastrutture di sistema e middleware;
  - analisi statica del codice sorgente o delle configurazioni di sistema;
  - disegno e valutazione dei sistemi di gestione per la sicurezza;
  - gestione processo di hardening di sistemi e piattaforme middleware;
  - validazione pattern di sviluppo sicuro del codice;
- capacità di comprendere l'infrastruttura sotto analisi e le relazioni tra i differenti sistemi;

- conoscenza approfondita delle diverse tipologie di attacco informatico, delle tecniche di penetration test, degli strumenti software utilizzati e dei più importanti tool ed exploit disponibili pubblicamente;
- esperienza nell'analisi delle vulnerabilità di sistemi e reti in esercizio senza impattare sull'operatività ed il funzionamento degli stessi;
- conoscenza complessiva delle problematiche di sicurezza dei dati e delle informazioni;
- **Certificazione OSSTMM Professional Security Tester (OPST) o Certified Etical Hacher (CEH)**.

4.5.6 **Senior Security Auditor**

Profilo

Laureato in discipline scientifiche con anzianità lavorativa di almeno 6 (sei) anni, da computarsi successivamente alla data di conseguimento del diploma di laurea, di cui almeno 3 (tre) anni di esperienza nella specifica funzione.

È richiesta, inoltre, in relazione alla tipologia di attività su cui verrà impiegata la risorsa:

- capacità di coordinamento dei Consulenti Junior;
- conoscenza dei processi e delle procedure operative IT;
- esperienza consolidata nella conduzione di IT Audit;
- conoscenza delle metodologie e delle linee guida ISO in materia di IT audit, e nell'applicazione delle stesse in funzione deli criteri di audit identificati;
- conoscenza delle linee guida ISO sui controlli di sicurezza in ambito enterprise e cloud ed esperienza nella contestualizzazione nel processo di mitigazione del rischio;
- esperienza consolidata nella valutazione di sistemi SGSI in accordo con la norma ISO:27001;
- conoscenza approfondita della normativa sulla Privacy e dei Provvedimenti del Garante sia in ambito Italiano che Europeo;
- conoscenza approfondita delle direttive dell'AgID i materia di sicurezza delle informazioni e continuità operativa dei servizi;
- esperienza consolidata nella valutazione di analisi di compliance in materia Privacy e direttive AgID su contesti analoghi, e nella definizione e governo dei piani di rientro;
- esperienza consolidata nella valutazione della documentazione a supporto per i processi di compliance al rispetto alle normative applicabili (es. Documento Programmatico della Sicurezza, Studio di fattibilità per la continuità operativa del CAD, ecc.);
- **certificazione CISA (Certified Information System Auditor)**.

4.5.7 **Senior Security Analyst**

Profilo

Laureato in discipline scientifiche con anzianità lavorativa di almeno 8 (otto) anni, da computarsi successivamente alla data di conseguimento del diploma di laurea, di cui almeno 4 (quattro) anni di esperienza nella specifica funzione.

È richiesta, inoltre, in relazione alla tipologia di attività su cui verrà impiegata la risorsa:

- capacità di coordinamento dei Consulenti Junior;
- conoscenza dei processi e delle procedure operative IT;
- conoscenza approfondita dei processi di Incident Handling ed Escalation per la gestione degli incidenti di sicurezza informatica;
- conoscenza approfondita dei processi di analisi forense, acquisizione degli elementi probatori e conservazione degli stessi;
- conoscenza approfondita dei sistemi di rilevazione e analisi degli allarmi;
- esperienza consolidata nell'analisi tecnica di incidenti all'interno di strutture SOC o CERT nell'ambito della Pubblica Amministrazione;
- esperienza consolidata nella gestione delle attività di supporto agli organi di Polizia Giudiziaria in caso di illeciti informatici;
- esperienza consolidata nella definizione proattiva di configurazioni e analisi di sicurezza;
- esperienza nella definizione di regole di correlazione e nel tuning delle stesse;
- conoscenza dei processi di reverse engineering dei malware ed esperienza consolidata nella analisi forense di malware mediante strumenti di analisi e attività di reverse;
- conoscenza approfondita dei protocolli di rete e della tipologia di traffico all'interno di un contesto complesso con esperienza consolidata nell'analisi forense del traffico di rete e nell'identificazione di anomalie o elementi a supporto per la corretta gestione degli incidenti di sicurezza.

4.5.8 **Junior Security Analyst**

Profilo

Laureato o Diplomato in discipline scientifiche con anzianità lavorativa di almeno 2 (due) anni di cui almeno 1 (uno) anni di esperienza nella specifica funzione.

È richiesta, in relazione alla tipologia di attività su cui verrà impiegata la risorsa:

- conoscenza dei processi e delle procedure operative IT;
- conoscenza dei processi di Incident Handling ed Escalation per la gestione degli incidenti di sicurezza informatica;
- conoscenza dei sistemi di rilevazione e analisi degli allarmi;
- esperienza nell'analisi tecnica di incidenti;
- conoscenza della modalità di intervento sulle postazioni client e sui server in caso di diffusione di malware di nuova generazione;

- conoscenza dei protocolli di rete e della tipologia di traffico all'interno di un contesto IT.

4.5.9 **Inalterabilità della composizione del team di servizio**

Il Fornitore sarà tenuto a rendere disponibili per lo svolgimento delle prestazioni contrattuali tutte le risorse indicate nella propria Offerta Tecnica, a non modificare la complessiva composizione del team di servizio proposto in Offerta Tecnica per l'intera durata del contratto, ed a garantire la disponibilità effettiva degli specialisti componenti il team di lavoro, rispettando il coinvolgimento dichiarato in fase di Proposta Tecnico Economica(**PTE**) o Piano di Lavoro (indicati rispettivamente ai paragrafi 5.3 e 5.4) , fatta salva la possibilità per la Committente e/o Amministrazione di richiederne la sostituzione.

5 MODALITÀ DI ESECUZIONE DELLA FORNITURA

5.1 Premessa

Le modalità di esecuzione, descritte in questo e nei successivi capitoli, potranno subire delle modifiche – anche in termini di semplificazioni o variazioni in funzione delle specificità dei singoli servizi/progetti/interventi - su proposta dell'Impresa e/o dell'Amministrazione/Committente, debitamente concordata.

La Committente e/o l'Amministrazione si riserva di chiedere al Fornitore di utilizzare prodotti o modulistica specifica di supporto alla gestione delle attività della fornitura (ad esempio: registrazione errori, log interventi, richiesta attività, ecc.).

La Committente e/o l'Amministrazione si riserva, inoltre, di avvalersi di soggetti terzi per il supporto allo svolgimento di attività di propria competenza.

Si sottolinea che al Fornitore è richiesto, in tutte le attività, il rispetto dei processi, degli standard e delle linee guida adottate dalla Committente e/o dall'Amministrazione; il Fornitore deve farsi carico, inoltre, di conoscere e diffondere al proprio interno tali conoscenze, di applicarle proattivamente e di recepirne tempestivamente eventuali variazioni.

5.2 Modalità di esecuzione dei servizi e delle attività

Al fine di descrivere le modalità di esecuzione della Fornitura, di seguito viene esposta la matrice di corrispondenza tra i servizi e le modalità di esecuzione.

Ambito	Servizio	Modalità di esecuzione
Security Consulting	Servizi on demand	Progettuale
	Incident Response Team	Continuativa

Tabella 5- Modalità di esecuzione dei servizi

Si sottolinea che, a prescindere dall'organizzazione adottata dal Fornitore per l'erogazione dei diversi servizi, è richiesto un alto grado di sinergia delle risorse messe a disposizione dal Fornitore operanti presso la Corte dei conti, al fine di garantire un adeguato grado di omogeneità nelle varie soluzioni adottate e uniformità di comportamento nei confronti degli utenti.

L'erogazione dei servizi deve comunque prevedere un alto grado di responsabilizzazione delle risorse del Fornitore, attitudine a lavorare per obiettivi, capacità di operare in team e rispetto delle scadenze pianificate.

Inoltre, nell'erogazione dei servizi è richiesto al Fornitore l'utilizzo, per l'intera durata del contratto, degli strumenti adottati da Corte dei conti per la gestione dell'operatività come a titolo esemplificativo ma non esaustivo il servizio cloud Service Now per l'IT service Management.

5.3 Modalità progettuale

I servizi di Security Consulting erogati in modalità progettuale, di cui al paragrafo 4.2, dovranno essere definiti, concordati e attivati a seguito della Data di Attivazione di cui al successivo par. 5.4 e sempre a fronte di una richiesta specifica da parte della Committente e/o dell'Amministrazione che verrà inviata – tramite mail o fax – al Responsabile del Contratto del Fornitore, contenente le seguenti informazioni di riferimento:

- data prevista di inizio attività;
- data prevista di fine attività;
- eventuali date vincolo (ad esempio legate a date di esercizio);
- tipologia di servizio richiesto;
- obiettivi e ambito di intervento;
- eventuali riferimenti a documentazione esistente;
- deliverable attesi (output dei vari work package);
- modalità operativa di intervento (on-site, entità interne ed esterne da coinvolgere e modalità di interazione con le stesse, frequenza di aggiornamento dei SAL, ecc.);
- milestone dell'intervento e tempistiche richieste per il rilascio dei vari work package;

A fronte della ricezione di una specifica richiesta da parte della Committente e/o dell'Amministrazione, vi sono due possibili modalità di gestione:

- caso in cui il Responsabile Tecnico del Fornitore – entro 3 giorni lavorativi dalla ricezione della richiesta dell'Amministrazione/Committente, non fa pervenire a queste ultime alcuna richiesta di chiarimenti/approfondimenti.

  In tale ipotesi, si intende tacitamente accettata la richiesta pervenuta e l'Impresa si obbliga a presentare entro ulteriori 3 giorni lavorativi, alla Committente e/o Amministrazione, una Proposta Tecnico Economica (PTE);

- caso in cui il Responsabile Tecnico del Fornitore – entro 3 giorni lavorativi dalla ricezione della richiesta dell'Amministrazione/Committente, fa pervenire a queste ultime una richiesta di chiarimenti/approfondimenti per chiarire l'ambito di intervento e le sue finalità e concordare la modalità operativa più idonea per garantire il risultato con la miglior efficienza ed efficacia possibile.

  In tale ipotesi, la Committente/Amministrazione si impegna a fornire al Responsabile Tecnico del Fornitore, che in ogni caso supporterà attivamente l'Amministrazione/Committente a tal fine, i chiarimenti e/o le informazioni richieste entro 5 giorni lavorativi. Alla data di ricezione degli stessi, il Fornitore redigerà e sottoporrà alla Committente/Amministrazione, entro i successivi 3 giorni lavorativi, una Proposta Tecnico Economica (PTE). Laddove, a fronte della ricezione dei menzionati chiarimenti e/o informazioni, il Fornitore ritenga necessario ottenere un ulteriore chiarimento, quest'ultimo provvederà tempestivamente a segnalare il fatto all'Amministrazione/Committente al fine di concordare in buona fede i necessari aggiustamenti. Le operazioni di condivisione saranno formalizzate in un apposito verbale sottoscritto da entrambe le parti. In tale ultimo caso i 3 giorni lavorativi per la redazione del PTE, decorreranno dalla data di sottoscrizione del verbale.

La Proposta Tecnico Economica (**PTE**) riporterà almeno i seguenti elementi:

- data prevista di inizio attività;
- data prevista di fine attività;
- il dettaglio delle attività che verranno fornite;
- possibili metodologie applicabili al contesto e la modalità di esecuzione delle attività;
- eventuali semilavorati che possono essere messi a disposizione della Committente/Amministrazione prima della accettazione formale della PTE;
- la lista completa dei deliverables (anche in termini di documentazione rilasciata, report o verbali di consegna, o altri elementi che certifichino la conclusione di uno specifico work package, all'interno del piano complessivo);
- le risorse coinvolte e il relativo effort : in particolare è prevista la presentazione di un team di lavoro i cui profili dovranno soddisfare quelli riportati nel paragrafo 4.5 (nell'ambito dei servizi on Demand) e che il Fornitore dovrà impiegare nelle varie aree di servizio richieste, definendo esplicitamente la percentuale di impiego riportata nel modello organizzativo proposto;
- il piano di lavoro dell'intero intervento sotto forma di gantt delle attività, evidenziando i vari work-package e le milestone di progetto.

A fronte di una PTE la Committente e/o l'Amministrazione potrà chiedere eventuali delucidazioni sulla modalità operativa di svolgimento e sui deliverable proposti al Responsabile del Contratto e/o al Responsabile Tecnico, richiedendo eventualmente la rivisitazione dell'intervento o l'attivazione solo di specifici work package o servizi all'interno dello stesso. A fronte dell'eventuale richiesta di rivisitazione/modifica, il Fornitore dovrà riproporre la PTE aggiornata entro 3giorni lavorativi, dalla data di richiesta della Committente e/o l'Amministrazione.

Nell'ambito della presentazione della PTE, il Fornitore dovrà descrivere anche il modello organizzativo che sarà adottato per garantire in maniera efficace ed efficiente sia il processo di attivazione delle richieste di intervento, sia l'esecuzione degli interventi stessi ponendo attenzione alla modalità di costituzione del/i gruppo/i di lavoro, le modalità di coordinamento degli stessi e il modello di pianificazione, controllo e comunicazione verso la Committente e/o l'Amministrazione, sullo stato di avanzamento dei vari interventi.

La Committente e/o l'Amministrazione potrà chiedere anche più interventi su ambiti diversi all'interno della stessa richiesta, in tal caso la PTE dovrà includere tutti gli interventi differenziati per aree di intervento/tipologia, riportando per ciascuno di essi le informazioni precedentemente illustrate.

Il dimensionamento di ciascun intervento è effettuato in giorni persona per ciascuna figura professionale prevista e costituisce un riferimento fisso ai fini del calcolo dei corrispettivi.

Tutte le attività di ingaggio iniziale e predisposizione degli interventi precedenti alla accettazione della PTE saranno a carico del Fornitore.

Una volta accettata formalmente la PTE di riferimento da parte dell'Amministrazione/Committente, l'Impresa dovrà attivare il servizio entro la data di prevista attivazione dell'intervento indicata nella PTE e garantire la pianificazione proposta, incluso il rilascio dei deliverable concordati e la rispondenza degli stessi agli obiettivi dell'intervento. Su questi ultimi parametri saranno misurati i livelli di servizio di fornitura dei Servizi On Demand e applicate le penali di riferimento in caso di mancato rispetto delle pianificazioni o non coerenza e non completezza dei deliverable rispetto agli obiettivi iniziali.

Nel caso in cui, durante l'esecuzione dell'intervento, siano richieste modifiche, il Fornitore può proporre una variazione della stima dell'effort progettuale da sottoporre all'approvazione della Committente/Amministrazione. In assenza dell'approvazione espressa i servizi saranno erogati nelle modalità precedentemente concordate.

Durante l'esecuzione del contratto, la Committente e/o l'Amministrazione potrà eseguire degli audit mirati a verificare la corrispondenza dei deliverable rispetto alle PTE attivate nel precedente periodo di esercizio e l'efficacia degli stessi rispetto agli obiettivi inizialmente concordati.

5.4 Modalità continuativa

A seguito della stipula del contratto, ai fini dell'attivazione dei servizi in modalità continuativa la Committente/Amministrazione potrà inviare – tramite mail o fax - una **Scheda di attivazione entro 10 giorni lavorativi** verso il Fornitore nella quale sono riportate le esigenze della Committente/Amministrazione.

L'Impresa, entro 5 giorni lavorativi dal ricevimento della suddetta Scheda di attivazione, dovrà redigere ed inviare alla Committente/Amministrazione il **Piano di Lavoro**, contenente le rispondenze alle esigenze espresse e l'indicazione a preventivo del team di lavoro (stimato sia in termini di effort, sia di date di completamento), i cui profili dovranno soddisfare quelli riportati nel paragrafo 4.5 (relativamente ai Servizi Continuativi) nonché la percentuale esplicita di impiego delle medesime.

La Committente/Amministrazione, ricevuto il **Piano di Lavoro**, potrà alternativamente:

a) accettarlo, senza alcuna richiesta di modifica e/o integrazione;

b) richiedere, secondo la procedura che segue e per non più di due volte, delle modifiche. Quest'ultime dovranno essere richieste entro il termine di 5 giorni lavorativi dal ricevimento del Piano di Lavoro e l'Impresa avrà ulteriori 5 giorni lavorativi dalla richiesta per sottoporre alla Committente/Amministrazione il Piano di Lavoro modificato.

L'approvazione, da parte della Committente/Amministrazione, del Piano di Lavoro determinerà l'attivazione dei servizi sopra richiamati: in particolare sarà considerata quale "**Data di Attivazione**" il primo giorno lavorativo utile, successivo alla data di approvazione del Piano di Lavoro.

Tutte le attività di ingaggio iniziale e predisposizione degli interventi precedenti alla approvazione del Piano di Lavoro saranno a carico del Fornitore.

Durante l'esecuzione dei servizi in modalità continuativa la Committente e/o l'Amministrazione potrà adeguare il perimetro di intervento incrementando o diminuendo il dimensionamento, fino alla sospensione del servizio specifico. Il Fornitore dovrà per ogni richiesta pervenuta di nuovo dimensionamento soddisfare i tempi di intervento richiesti dalla Committente e/o dell'Amministrazione e comunque non oltre 5 giorni lavorativi dalla ricezione della richiesta, riadeguando il Piano di Lavoro.

Nel caso eventuale di totale sospensione del servizio specifico, la riattivazione sarà formalizzata da parte della Committente/Amministrazione attraverso l'invio di una nuova Scheda di attivazione, in modo analogo a quanto già sopra indicato (ovviamente senza alcun effetto sulla Data di Attivazione, che rimarrà immutata).

In nessun caso potrà essere modificato il Piano di Lavoro senza previa espressa approvazione della Committente/Amministrazione.

La Committente e/o Amministrazione potrà richiedere a fronte di esigenze estemporanee la presenza di una o più risorse con profilo Junior Security Analyst e/o Senior Security Analist. Tale richiesta dovrà essere soddisfatta entro 15 giorni lavorativi dalla ricezione della richiesta.

Durante l'esecuzione del contratto, la Committente e/o l'Amministrazione potrà eseguire degli audit mirati a verificare la corrispondenza dei deliverable rispetto al Piano di Lavoro concordato.

5.5 Gestione della Fornitura

L'esecuzione ed il governo della Fornitura dovrà avvenire con un'attività continua di pianificazione, consuntivazione e controllo. All'inizio della Fornitura, la Committente e/o l'Amministrazione illustrerà le attività da svolgere, indicando le informazioni e le scadenze note, i piani di evoluzione e ogni altra informazione utile ad una corretta pianificazione (per le attività cui la pianificazione sia applicabile).

In ogni caso sarà cura del Fornitore predisporre e aggiornare tempestivamente le proprie attività, in funzione delle variazioni intervenute, in modo da riflettere il reale stato delle attività, a preventivo e a consuntivo.

La Committente si riserva di accedere in ogni momento a tali pianificazioni o a richiederne opportuna documentazione, al fine di condividere in tempo reale con il Fornitore lo stato delle attività della Fornitura.

A tal proposito, il Fornitore dovrà mantenere aggiornato mensilmente lo stato di avanzamento dei lavori (SAL), fornendo tempestivamente indicazioni sulle attività concluse ed in corso, esplicitandone la percentuale di avanzamento, su eventuali criticità/ritardi, su azioni di recupero e razionali dello scostamento.

5.6 Consuntivazione

La consuntivazione delle attività è predisposta periodicamente, su base mensile, attraverso la documentazione di rendicontazione inclusa nel documento di "**Resoconto Attività**", sia in termini di volumi sia di andamento dei servizi e delle attività. Le eventuali osservazioni della Committente sui contenuti di tali documenti saranno effettuate in forma scritta, attraverso e-mail nonché attraverso lettere di rilievo, fermo restando che le informazioni e i dati di cui al Resoconto Attività saranno successivamente vagliati dalla Committente in sede di verifica di conformità.

5.7 Controllo

E' richiesto che il Fornitore operi il controllo costante e diretto delle condizioni e dei processi di erogazione dei servizi, supportando la Committente e/o l'Amministrazione nel governo e nell'evoluzione dei servizi stessi.

Il Fornitore, inoltre, deve fornire alla Committente e/o all'Amministrazione gli elementi per il costante miglioramento dei servizi nonché comunicare tempestivamente eventuali elementi di criticità e/o situazioni fuori linea.

5.8 Trasferimento del know-how

Negli ultimi due mesi solari di validità del contratto, o nel caso di cessazione anticipata del rapporto contrattuale, il Fornitore, su richiesta della Committente, deve fornire al personale della Committente e/o dell'Amministrazione, o a terzi designati, il trasferimento del know-how sulle attività condotte, al fine di rendere l'eventuale prosecuzione delle attività quanto più efficace possibile. Pertanto, il Fornitore si impegna:

- a trasferire il know how necessario, nonché l'eventuale supporto operativo, alla presa in carico degli strumenti resi disponibili dall'Amministrazione;
- a facilitare la presa in carico da parte del Fornitore subentrante anche attraverso la disponibilità ad eseguire attività operative.

Al termine delle attività contrattuali, la documentazione prodotta/modificata nell'ambito dell'appalto sarà consegnata alla Committente secondo le modalità che saranno concordate.

Tale periodo di affiancamento è organizzato secondo quanto previsto nell'ambito dell'Offerta Tecnica presentata in gara dall'Impresa, nonché secondo le modalità eventualmente concordate con la Committente e/o con l'Amministrazione.

Le attività di trasferimento del know how si intendono ricomprese nel corrispettivo dei servizi.

6 VERIFICA DI CONFORMITÀ

Per quanto attiene alle verifiche di conformità si rimanda all'articolo 12 S dell'allegato 4 "Schema di Contratto condizioni Speciali".

7 INDICATORI DI QUALITÀ

Di seguito viene descritto un insieme minimo di requisiti di qualità della Fornitura e delle relative modalità di verifica e controllo. Il Fornitore è tenuto, per l'intera durata dei servizi, a rendicontare gli indicatori di qualità (IQ).
Si precisa che:

- per periodo di riferimento si intende l'arco di tempo entro il quale sono rilevate le grandezze necessarie per la determinazione dei requisiti di qualità. E' specificato per ogni indicatore di qualità (IQx);
- per ore e giorni si intendono ore lavorative e giorni lavorativi;
- per mese, trimestre, semestre, si indica il mese, il trimestre, il semestre di calendario nell'ambito della durata contrattuale.

Ai fini della misurazione degli indicatori di qualità, si precisa che, eventuali centesimi dei valori percentuali rilevati dovranno essere arrotondati ad una unica cifra decimale:

- per difetto se i centesimi sono < 5;
- per eccesso se i centesimi sono >= 5.

Ad esempio:
15,06% diventa 15,1%;
10,01% diventa 10,0%;
10,49% diventa 10,5%;
14,98% diventa 15,0%.

Si precisa che agli Indicatori di Qualità sono, di volta in volta, associate azioni contrattuali quali l'applicazione di penali.

7.1 IQ1: SOSTITUZIONE DEL RESPONSABILE TECNICO DELLA FORNITURA

Aspetto da valutare	Sostituzione del Responsabile tecnico della Fornitura operata su iniziativa dell'Impresa e non a fronte di richiesta della Committente e/o dell'Amministrazione.		
Unità di misura	Responsabili sostituiti	**Fonte dati**	Lettera di sostituzione del Responsabile tecnico della Fornitura da parte del Fornitore
Periodo di osservazione	Semestre precedente la rilevazione	**Frequenza di misurazione**	Semestrale
Dati da rilevare	• Sostituzione permanente del Responsabile tecnico della Fornitura non richiesta da Committente e/o dall'Amministrazione(*Nsostituzioni*)		
Regole di campionamento	Vanno considerate le sostituzioni non richieste dalla Committente e/o dall'Amministrazione che riguardano il Responsabile tecnico della Fornitura.		
Formula	IQ1= *NSostituzioni*		
Regole di arrotondamento	Nessuna		
Valore di soglia	IQ1 = 0		
Azioni contrattuali	Applicazione delle penali come indicato nello schema di contratto.		

7.2 IQ2: PERSONALE DELLA FORNITURA INADEGUATO

Aspetto da valutare	Personale della Fornitura inadeguato		
Unità di misura	Richiesta di sostituzione	**Fonte dati**	E-mail, lettere, verbali
Periodo di riferimento	Semestre precedente la rilevazione	**Frequenza di misurazione**	Semestre
Dati elementari da rilevare	Numero di sostituzioni, richieste formalmente da Committente/Amministrazione, del personale della Fornitura (N_Sostit_rich).		
Regole di campionamento	Vanno considerate le sostituzioni richieste da Committente/Amministrazione che riguardano il personale della Fornitura nel periodo di riferimento.		
Formula	IQ2 = *N_Sostit_rich*		
Regole di arrotondamento	Nessuna		
Valore di soglia	IQ2 <= 2		
Azioni contrattuali	Applicazione delle penali come indicato nello schema di contratto.		

7.3 IQ3: TURN OVER DEL PERSONALE

Aspetto da valutare	Turn over del personale: numero di risorse sostituite su iniziativa del Fornitore nel periodo di riferimento.		
Unità di misura	Risorsa sostituita	**Fonte dati**	E-mail, lettere, verbali
Periodo di riferimento	Semestre precedente la rilevazione	**Frequenza di misurazione**	Semestrale
Dati elementari da rilevare	Numero di sostituzioni effettuate su iniziativa del Fornitore nel periodo di riferimento (N_Sostit).		
Regole di campionamento	Nessuna		
Formula	IQ3 = N_Sostit		
Regole di arrotondamento	Nessuna		
Valore di soglia	IQ3 <= 3		
Azioni contrattuali	Applicazione delle penali come indicato nello schema di contratto.		

7.4 IQ4: SLITTAMENTO DI UNA SCADENZA CONTRATTUALE

Aspetto da valutare	Il rispetto di ciascuna scadenza (inserimento/sostituzione risorse, di un deliverable, attivazione di un servizio/ fine attività di un servizio, ecc.) stabilita dal contratto e/o dal Piano di Lavoro e/o dalla PTE e/o di carattere trasversale ai servizi.		
Unità di misura	Giorno lavorativo	**Fonte dati**	E-mail, fax, verbali
Periodo di riferimento	Evento	**Frequenza di misurazione**	Giornalmente
Dati elementari da rilevare	• Data prevista (*data_prev*); • Data effettiva (*data_eff*).		
Regole di campionamento	Nessuna		
Formula	IQ4 = *data_eff- data_prev*		
Regole di arrotondamento	Nessuna		
Valore di soglia	IQ4 <= 0		
Azioni contrattuali	Applicazione delle penali come indicato nello schema di contratto.		

7.5 IQ5: QUALITÀ DELLA DOCUMENTAZIONE PRODOTTA

Aspetto da valutare	Riemissione dei documenti a seguito di rilievi emessi dalla Committente.		
Unità di misura	Punto percentuale	**Fonte dati**	Lettere di notifica al Fornitore di non approvazione del documento.
Periodo di riferimento	Semestre precedente la rilevazione	**Frequenza di misurazione**	Semestrale
Dati elementari da rilevare	Numero di documenti rielaborati (N_documenti_rielaborati) Numero di documenti consegnati (N_documenti)		
Regole di campionamento	Vanno considerati tutti i documenti consegnati nel periodo di riferimento		
Formula	IQ4= ((N_documenti_rielaborati)/(N_documenti))*100		
Regole di arrotondamento	La percentuale va arrotondata per eccesso alla prima cifra decimale		
Valore di soglia	IQ4 <= 5,0%		
Azioni contrattuali	Applicazione delle penali come indicato nello schema di contratto.		

7.6 IQ6: RILIEVI SULLA FORNITURA

Aspetto da valutare	Numero di rilievi emessi per inadempimenti sulla fornitura		
Unità di misura	Rilievo sulla fornitura	**Fonte dati**	Nota/e di rilievo
Periodo di riferimento	Trimestre precedente la rilevazione	**Frequenza di misurazione**	Semestrale
Dati da rilevare	Numero Rilievi emessi sulla fornitura (*Nrilievi_forn*)		
Regole di campionamento	Si considerano tutti i rilievi comunicati tramite nota/e di rilievo nel periodo di riferimento		
Formula	*RLFN = Nrilievi_forn*		
Regole di arrotondamento	Nessuna		
Valore di soglia	RLFN <= 3		
Azioni contrattuali	Applicazione delle penali come indicato nello schema di contratto.		

8 PENALI

Lo scopo delle penali è quello di riequilibrare il servizio effettivamente ricevuto (di minore qualità, e/o generando disservizi e/o ritardi e/o inducendo un danno all'utilizzatore) dalla Committente/Amministrazione al corrispettivo da erogarsi che è stabilito per prestazioni effettuate a regola d'arte.
Le penali da adottare sono individuate contrattualmente e normalmente sono organizzate in modo progressivo in relazione alla gravità o al ripetersi della mancata soddisfazione degli adempimenti richiesti.
Per il dettaglio del processo di contestazione ed applicazione delle penali, si rinvia a quanto puntualmente disciplinato nel contratto.