ALLEGATO 5
CAPITOLATO TECNICO

GARA A PROCEDURA APERTA AI SENSI DEL D.LGS. 163/2006 E S.M.I., PER L'ACQUISIZIONE DI SUPPORTO TECNICO-METODOLOGICO ALLE ATTIVITÀ DI AUDIT DELLA DIREZIONE CENTRALE PER I SERVIZI INFORMATIVI E TELECOMUNICAZIONE E ALLE ATTIVITA' DI CONTROLLO DELL'EFFICACIA DELLE MISURE DI SICUREZZA IT DELL'INAIL

INDICE

I. GLOSSARIO

Action Plan	Piano di lavoro ad alto livello riportante gli interventi tecnici ed organizzativi da porre in essere per far fronte alle non conformità, rischi, vulnerabilità, gap, ecc. in esito ad un'attività di analisi
Amministrazione	L'Istituto Nazionale per l'Assicurazione contro gli Infortuni sul Lavoro o INAIL
Benchmark CIS	Benchmark sviluppati dal Center for Internet Security che offrono informazioni di supporto alle organizzazioni e le assistono nell'operare scelte consapevoli con le opzioni di protezione disponibili per le diverse piattaforme tecnologiche
Deliverable	Risultato verificabile prodotto da un'attività progettuale; indica un oggetto materiale o immateriale prodotto come risultato di una attività del progetto.
DCSIT	La Direzione Centrale Servizi Informativi e Telecomunicazioni dell'INAIL
Effort	Quantità di lavoro necessaria a completare un'attività progettuale; normalmente espressa in giorni/uomo o mesi/uomo
Follow-up	Attività periodica di rivisitazione e valutazione del contenuto dei rapporti di audit e/o dei risultati di analisi precedenti, al fine di valutare se la direzione, funzione o settore è intervenuta, o sta intervenendo, in conformità al remediation plan sulle rischiosità / problematiche segnalate. La risposta della struttura interessata deve essere esaminata sia come elemento di valutazione dell'atteggiamento della struttura rispetto ai suggerimenti dati, sia come elemento di valutazione dell'efficacia degli interventi di audit e/o delle attività

	di analisi
Fornitore Aggiudicatario o Aggiudicatario	Il concorrente che risulta primo nella graduatoria definitiva
INTERNATIONAL PROFESSIONAL PRACTICES FRAMEWORK (Standards)	Standard definito dall' IIA (The Institute of Internal Auditors) per la conduzione degli internal audit. Contiene due tipi di authorative guidance: 1. I principi e linee guida vincolanti che includono: • Definizione di Internal Auditing; • Codice Etico; • Standard. 2. I principi e linee guida fortemente raccomandati che includono: • Position Paper; • Guide interpretative; • Guide pratiche.
ISO/IEC 27001	Lo standard internazionale ISO/IEC 27001 (Information technology – Security techniques – Information Security Management Systems – Requirements"),fornisce un modello per definire, realizzare, rendere operativo, monitorare, esaminare, mantenere e migliorare un sistema di gestione della sicurezza delle informazioni correttamente documentato. La ISO/IEC 27001 consente di valutare attentamente tutti i rischi riferibili al business e di evidenziare le aree in cui è necessario un miglioramento. Le modalità di protezione delle informazioni consistono nell'assicurarne adeguati livelli di riservatezza, integrità e accessibilità, attraverso la gestione controllata dei processi aziendali e ciò richiede l'utilizzo quindi di personale, procedure e sistemi IT
IT Audit	Processo di verifica della conformità dei sistemi informativi di un'organizzazione a quanto previsto da norme, regolamenti o pratiche interne
IT Risk Management	Insieme dei processi con cui un'azienda identifica, analizza, quantifica, elimina e monitora i rischi legati ai

	processi ICT
IT Security Audit	Processo di verifica della conformità della sicurezza dei sistemi informativi di un'organizzazione ai requisiti di sicurezza IT previsti da norme, regolamenti o pratiche interne
Riunione di Kick Off	Riunione formale per l'avvio ufficiale delle attività progettuali.
Minaccia	Potenziale evento dannoso perpetrato da fattori umani, naturali o tecnologici che può colpire gli asset posseduti dall'azienda
Piano di Audit	Descrizione delle attività e delle disposizioni per la conduzione di un' audit
Process Owner	Colui che si fa carico del risultato di un processo aziendale e ne presidia l'efficacia e l'efficienza complessiva
Risk Control Matrix	Modalità di rappresentazione, per ciascun processo analizzato, dei seguenti elementi: - rischio rilevato (potenziale e residuo) - obiettivi di controllo a presidio del processo - attività di controllo per il raggiungimento degli obiettivi di controllo - ambito di applicazione delle attività di controllo - adeguatezza delle attività di controllo - evidenza delle attività di controllo
Segregation of Duty	Il principio della separazione dei ruoli/attività, o SoD, è una delle regole cardine del modello organizzativo di un'azienda e, in particolare, costituisce uno dei principi generali di controllo interno. La SoD prevede che le responsabilità devono essere definite e debitamente distribuite evitando sovrapposizioni funzionali o

	allocazioni operative che concentrino le attività critiche su un unico soggetto
Vulnerabilità	Caratteristica intrinseca del sistema che può consentire ad una minaccia di concretizzarsi

II. ACRONIMI

AdS	Amministratori di Sistema, così come definiti nel provvedimento emanato dal Garante per la protezione dei dati personali il 27 Novembre 2008, recante misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema
CIS	Center for Internet Security; organizzazione no-profit focalizzata sul miglioramento della Cyber Security in ambito pubblico e privato
CoSO ERM Framework	Framework definito dal **C**ommittee **o**f **S**ponsoring **O**rganizations of the Treadway Commission per l'**E**nterprise **R**isk **M**anagement. Il framework fornisce una definizione della gestione del rischio aziendale e ne descrive i principi e i concetti. Fornisce una guida per tutti i livelli del management, che operano sia nelle imprese che in altre organizzazioni, per valutare e accrescere l'efficacia del processo di gestione del rischio; utilizzato per la formulazione delle strategie in tutta l'organizzazione; progettato per individuare eventi potenziali che possono influire sull'attività aziendale, per gestire il rischio entro i limiti del rischio accettabile e per fornire una ragionevole sicurezza sul conseguimento degli obiettivi aziendali
DCSIT	Direzione Centrale Servizi Informativi e Telecomunicazioni dell'INAIL
FTE	Full Time Equivalent; viene principalmente utilizzato per indicare lo sforzo erogato o pianificato per svolgere una attività o un progetto. Un FTE equivale ad una persona che lavora a tempo pieno (8 ore al giorno) per

	un anno lavorativo
HR	Generalmente utilizzato per indicare la funzione Human Resources, ovvero la funzione deputata alla gestione delle Risorse Umane in un'azienda
ICT	Information & Communication Technology
IP	Indici di prestazione
IPPF	l'INTERNATIONAL PROFESSIONAL PRACTICES FRAMEWORK definite dall'Institute of Internal Auditors
IQ	Indice di Qualità
NIST	L'istituto statunitense degli standard e della tecnologia derivato dal precedente National Bureau of Standards
NIST-SP800-115	Technical Guide to Information Security Testing and Assessment rilasciata dal NIST; è una guida agli aspetti tecnici di base per la conduzione delle attività di verifica della sicurezza dell'informazione
OSSTMM	Open Source Security Testing Methodology Manual; nel corso degli anni è divenuto lo standard internazionale di riferimento per l'esecuzione di verifiche di sicurezza. La metodologia OSSTMM definisce esattamente quali elementi devono essere verificati, che cosa occorre fare prima, durante e dopo i test di sicurezza e come misurare i risultati ottenuti. Essa non indica esplicitamente gli strumenti da impiegare durante le verifiche, ma dettaglia i metodi da utilizzare per valutare sul campo in modo consistente e ripetibile la superficie di attacco relativa al contesto oggetto di analisi. La metodologia OSSTMM fornisce, inoltre, una metrica accurata per valutare il livello di sicurezza operativa del contesto oggetto di analisi
PT	Penetration Test

SGSI	Sistema di gestione della sicurezza delle informazioni
SoD	Segregation of Duty
Userid	Identificativo dell'utente con il quale viene riconosciuto da un computer, da un programma o da un server
VA	Vulnerability Assessment

1. INTRODUZIONE

Il presente capitolato è parte integrante della documentazione di gara e definisce le caratteristiche e i requisiti per l'affidamento di servizi professionali volti a supportare le attività della Direzione Centrale Servizi Informativi e Telecomunicazioni (nel seguito DCSIT) dell'INAIL.

Le prescrizioni del presente capitolato rappresentano i requisiti minimi dell'affidamento.

2. CONTESTO DI RIFERIMENTO

Le attività svolte dalla Direzione Centrale Servizi Informativi e Telecomunicazioni nell'ambito ICT dell'INAIL possono essere ricondotte a due aree:

1. gestire l'evoluzione dei sistemi informatici;
2. garantire l'esercizio degli stessi sistemi.

Il modello di riferimento adottato dall'Amministrazione, con riferimento all'IT, prevede di mantenere in capo alla Direzione la fase di governo nello sviluppo di una iniziativa IT,ovvero di mantenere le fasi a più elevato valore aggiunto: dalla comprensione del fabbisogno, dalla pianificazione dei singoli task al complessivo controllo progettuale - cedendo, invece, al mercato della fornitura le fasi operative/realizzative e di conduzione.

Con l'obiettivo di potenziare il proprio ruolo di governo sui processi di business ad essa riconosciuti, la DCSIT ha adottato un nuovo modello organizzativo volto a:

- individuare specifiche responsabilità a copertura di alcune fasi critiche della catena del valore orientate al governo e alla qualità dei servizi;
- potenziare un sistema di controlli per gestire sistematicamente le disfunzioni o le irregolarità che potrebbero ostacolare il raggiungimento degli obiettivi della Direzione.

L'attuale struttura organizzativa della DCSIT, pertanto, prevede un assetto organizzativo orientato ai servizi e ai progetti, con il supporto di funzioni trasversali centralizzate tra le quali si collocano la Funzione Sicurezza e la Funzione Monitoraggio e audit IT.

A tali funzioni viene riconosciuta la responsabilità di:

- garantire l'adeguatezza dei processi finalizzati al miglioramento dell'efficacia e dell'efficienza dell'organizzazione e assistere la DCSIT nel perseguimento dei propri

obiettivi, ottimizzando i processi di controllo, di gestione dei rischi e di conformità dei servizi erogati;

- definire strategie e policy di sicurezza, verificare l'efficacia e la congruità del Sistema per la Gestione della Sicurezza delle Informazioni e monitorare l'adeguatezza delle contromisure e degli standard di sicurezza ICT

3. DESCRIZIONE DELLA FORNITURA E OGGETTO DELLA STESSA

L'oggetto della fornitura, le caratteristiche relative all'organizzazione e alle modalità di svolgimento descritto nei successivi paragrafi, si articola in due lotti, uno per ciascun ambito di intervento:

- **Lotto 1** - **Supporto tecnico-metodologico alle attività di Audit IT**:

  i cui servizi sono così articolati:

  a. Valutazione e gestione dei rischi IT;
  b. Esecuzione delle attività di audit IT;
  c. Supporto specialistico per l'attività di Indirizzo e coordinamento della funzione di AUDIT.

- **Lotto 2** - **Controllo dell'efficacia delle misure di sicurezza IT**

  i cui servizi sono così articolati:

  a. IT Security Audit;
  b. Analisi delle attività degli Amministratori di Sistema;
  c. ICT Security Assessment.

Si precisa che, in assenza di espliciti riferimenti ad uno specifico lotto, quanto stabilito nei capitoli seguenti è **valido per entrambi i lotti della fornitura.**

3.1. Lotto 1: Supporto tecnico-metodologico alle attività di Audit IT

3.1.1. Contesto di riferimento – Lotto 1

Alla funzione Monitoraggio e audit IT sono riconosciute, in sintesi, le seguenti aree di responsabilità:

- Progettazione, e gestione del sistema di audit IT;
- Pianificazione delle attività e degli interventi di audit, conduzione degli interventi, redazione dei rapporti di audit e analisi e individuazione di azioni correttive;
- Valutazione e monitoraggio del livello dei rischi indotti, del livello di aderenza dei processi agli standard operativi e di qualità definiti.

In tale contesto e in relazione al ruolo ad esso riconosciuto nell'ambito della DCSIT, la funzione di Monitoraggio e audit IT ha l'esigenza di avvalersi di un servizio di assistenza specializzata per:

a) definire il modello di valutazione del rischio e le relative procedure e metodologie di applicazione e reiterazione nel corso del tempo;
b) essere supportato nelle attività di audit e di formalizzazione dei risultati;
c) supportare le attività di indirizzo e coordinamento della Funzione Monitoraggio e audit IT.

3.1.2. Perimetro della fornitura – Lotto 1

Per lo svolgimento della propria missione istituzionale la DCSIT agisce secondo un modello funzionale che trova la propria rappresentazione nella "catena del valore della DCSIT".

La catena del valore che, fornisce, a livello macro, una visione sulle attività svolte in DCSIT, rappresenta, dunque, le "aree di processo" mediante le quali l'intera Direzione svolge il suo ruolo di supporto a tutte le altre unità organizzative di INAIL, garantendo l'erogazione di servizi IT costantemente allineati con le esigenze di business e nel rispetto dei livelli di servizio concordati.

In Figura 1 è rappresentata la "catena del valore della DCSIT".

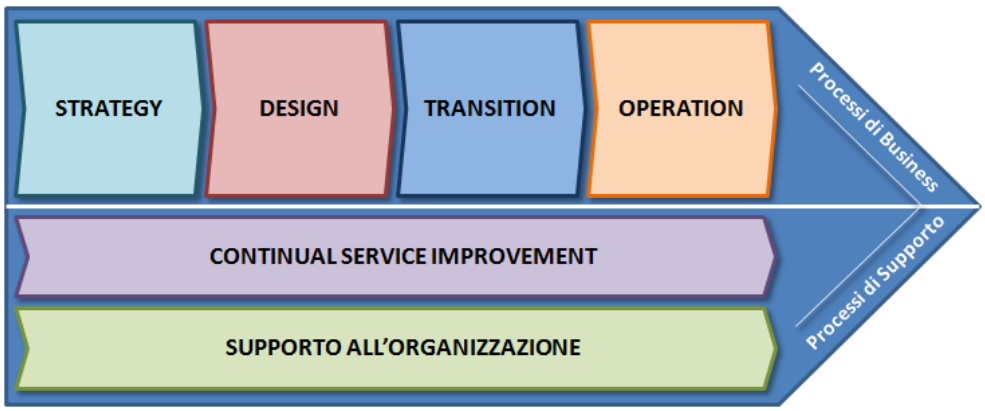


Figura 1 - Catena del valore della DCSIT

Al suo interno vengono individuate 2 tipologie di aree:

- processi di business, finalizzati a raggiungere la missione della DCSIT;
- processi di supporto, mirati a sostenere l'operatività della struttura.

Le aree descritte nella Catena del Valore della DCSIT sono mutuate dalle corrispondenti fasi del framework ITIL V3 - Service Strategy, Service Design, Service Transition, Service Operations e Continual Service Improvement, con l'aggiunta dell'area Supporto all'Organizzazione per tener conto di processi specifici di natura amministrativa e di supporto al funzionamento dell'intera organizzazione.

Le suddette aree che forniscono una visione complessiva delle macroattività della DCSIT sono esplose in processi di maggior dettaglio su due livelli sottostanti, rappresentati dai macro processi e dai processi[1]. Il secondo livello, pertanto, è quello dei **"macro-processi"**, che raffigura una scomposizione degli elementi chiave costituenti ciascuna area e introduce una rappresentazione più analitica delle singole aree. Il macro-processo e', dunque, l'elemento che consente di raccordare i processi che operano in ambiti omogenei.

Il terzo e ultimo livello, infine, contiene la scomposizione in singoli processi il cui significato è conforme a quanto tradizionalmente previsto.

[1] Quanto detto è definito e rappresentato nel documento "Modello dei processi della DCSIT" che sarà consegnato al fornitore aggiudicatario in sede di avvio delle attività progettuali.

L'intervento in oggetto riguarderà esclusivamente i processi di business, rappresentati nella parte alta dello schema grafico, attraverso i quali si svolgono le attività connesse al raggiungimento della funzione core della DCSIT.

A titolo indicativo, ma non vincolante per l'Amministrazione, in quanto tutt'ora in corso la progettazione di dettaglio dei singoli processi, il perimetro dell'intervento, riportato in

Tabella 1, è rappresentato da 28 macro processi dettagliati in 53 processi la cui documentazione di dettaglio sarà resa disponibile all'Aggiudicatario in sede di avvio delle attività.

Si precisa che i 53 processi in perimetro sono sotto la responsabilità di 10 process owner.

AREA	MACRO PROCESSO	N° PROCESSI
Service Strategy	Sviluppo della Strategia	2
	Pianificazione e Controllo della Gestione IT	2
	Gestione del Portafoglio dei Servizi	3
	Gestione della Domanda	1
Service Design	Gestione del Catalogo dei Servizi	1
	Gestione del Livello di Servizio	3
	Gestione della Capacità dei Servizi e dell'Infrastruttura IT	1
	Gestione della Disponibilità	2
	Gestione della Continuità dei Servizi IT	2
	Gestione della Sicurezza delle Informazioni	3
	Gestione del Fornitore	4
	Definizione Studi, Analisi e Requisiti	1
	Definizione ed Evoluzione delle Architetture di Riferimento	1
Service Transition	Coordinamento delle Attività di Pre Esercizio	1
	Validazione e Test del Servizio	3
	Gestione dei Rilasci in Esercizio	3
	Gestione dei Cambiamenti	1
	Gestione della Configurazione	2
	Valutazione servizi IT	1
	Gestione della Conoscenza	2
	Pianificazione e Controllo Interventi Progettuali	1
	Evoluzione e Sviluppo Servizi IT	3
	Monitoraggio	2
Service Operation	Gestione degli Eventi	1

AREA	MACRO PROCESSO	N° PROCESSI
	Gestione delle Eccezioni	**2**
	Gestione degli Accessi	**1**
	Gestione delle Segnalazioni Utente	**1**
	Gestione dell'IT Operation	**3**

Tabella 1- Perimetro d'intervento - Lotto 1

3.1.3. Oggetto della fornitura – Lotto 1

Limitatamente ai processi e alle procedure individuati nel perimetro oggetto della presente fornitura, la DCSIT ha deciso di avvalersi di un supporto specialistico per svolgere le seguenti attività, dettagliate nei paragrafi a seguire:

3.1.3.1 – Valutazione e gestione dei rischi IT;

3.1.3.2 – Esecuzione delle attività di IT Audit;

3.1.3.3 -Supporto specialistico per l'attività di indirizzo e coordinamento della Funzione Monitoraggio e audit IT.

A seguito dell'assegnazione delle attività l'Aggiudicatario dovrà predisporre un piano di lavoro della fornitura, in accordo con la Funzione Monitoraggio e audit IT, che ne potrà chiedere la rimodulazione, comprendente le attività di controllo previste. Il piano di lavoro della fornitura dovrà essere predisposto in modo tale da organizzare l'insieme dei servizi secondo un ordine di priorità che tenga conto:

- delle esigenze strategiche ed operative dell'Amministrazione;
- delle aree di attività che risultano maggiormente critiche sulla base dell'attuale situazione e delle esigenze future (evoluzioni organizzative, possibili cambiamenti operativi, ecc.);
- della necessità di articolare le varie attività di IT Audit secondo criteri di efficienza e di creazione di possibili sinergie.

Si precisa che è richiesta all'Aggiudicatario la predisposizione, secondo le tempistiche riportate in

Tabella **2** e in coerenza con il piano di lavoro della fornitura, del piano di lavoro per il singolo servizio richiesto (piano di lavoro del servizio) che dovrà essere condiviso ed approvato dalla Funzione Monitoraggio e audit IT.

Con riferimento al singolo servizio è previsto che l'Amministrazione ne comunichi formalmente l'avvio.

3.1.3.1. Valutazione e gestione dei rischi IT

L'attività si propone l'obiettivo di individuare, analizzare e valutare il rischio in ambito IT, ovvero di identificare rischi di disfunzioni o irregolarità nelle varie attività dei processi e procedure compresi nel perimetro dell'intervento (vedi paragrafo 3.1.2) e valutarne l'impatto potenziale.

Contestualmente, devono essere individuati i controlli previsti e messi in atto dai responsabili dei singoli processi (process owner) a mitigazione dei rischi stessi e finalizzati ad evitare che le disfunzioni o irregolarità si verifichino in concreto.

La metodologia proposta dal fornitore, di cui dovrà dare chiara ed esaustiva descrizione nell'Allegato 2 - Offerta Tecnica, dovrà basarsi sul framework CobIT 5, essere in linea con le best practice di settore e dovrà consentire di integrare i risultati delle attività di analisi e gestione del rischio con l'ERM COSO framework adottato dall'Amministrazione.

Per traguardare l'obiettivo preposto la metodologia proposta dall'impresa dovrà prevedere almeno le seguenti macro fasi progettuali:

1. **Analisi del contesto**: volta alla comprensione del modello di governo e gestione dell'ICT tramite l'analisi della documentazione di dettaglio dei processi IT inclusi nel perimetro dell'intervento e, più in generale, della documentazione utile a comprendere il contesto aziendale di riferimento;

2. **Analisi dei rischi:** ovvero l'identificazione, attraverso tecniche di "gathering" (interviste, questionari di rilevazione, ecc.), dei rischi, dei fattori che li determinano (minacce, vulnerabilità, fattori esterni, ecc.) e della stima qualitativa/quantitativa della probabilità di accadimento e del suo impatto sui diversi ambiti delle attività della DCSIT rientranti nel perimetro progettuale;

3. **Gestione dei rischi**: ovvero la valutazione del livello di esposizione ai rischi dei processi in perimetro, tramite l'applicazione dei razionali previsti dalla metodologia di Risk Management proposta dal fornitore, e la definizione della rischiosità residua complessiva di ciascun processo analizzato, mediante ponderazione del sistema di controllo dichiarato. La fase dovrà concludersi con l'individuazione delle opportune strategie, azioni e controlli da attuare per la rimozione o mitigazione del rischio rilevato.

Si evidenzia che le attività di analisi e gestione del rischio, da effettuare su tutti i processi

in perimetro, dovranno trovare compimento entro i primi 4 mesi di contratto a partire dalla data di avvio della fornitura e non dovranno essere reiterate nel secondo anno di fornitura.

Per quanto riguarda gli strumenti a supporto, si fa presente che il servizio dovrà essere gestito e documentato utilizzando, in alternativa, un tool di mercato, la cui valutazione da parte dell'Amministrazione è attualmente in corso, o prodotti di office automation che saranno messi a disposizione dell'aggiudicatario. In entrambi i casi l'Aggiudicatario verrà aggiornato sulla scelta effettuata dall'Amministrazione in occasione dell'incontro di avvio attività (kick-off).

DELIVERABLE ATTESI

I deliverable attesi in esito alle attività previste sono riepilogati di seguito:

- l'Executive Summary, riportante la sintesi dei risultati delle attività di analisi effettuate per una presentazione alla Direzione;
- i verbali delle interviste svolte, condivisi con i process owner, in cui siano descritti i processi analizzati ed i relativi rischi;
- i questionari di rilevazione compilati dai process owner;
- la Risk Control Matrix, riportante il dettaglio dei rischi individuati per ogni processo o procedura rientrante nel perimetro d'analisi, ed i relativi controlli in essere o gli eventuali gap rilevati. La Risk Control Matrix dovrà permettere di identificare e classificare rischi sia potenziali, sia residui;
- un Technical Report di raccomandazioni con evidenziati i punti di debolezza o di miglioramento individuati, che incorpora i piani di azione, concordati con il management di DCSIT;
- un Action Plan, con l'indicazione delle attività da svolgere, delle risorse da impiegare, delle tempistiche di massima previste per la realizzazione dei singoli interventi da porre in essere per la rimozione o mitigazione dei rischi rilevati.

I risultati dell'attività dovranno essere validati dalla Funzione Monitoraggio e audit IT della DCSIT e condivisi e illustrati al Direttore Centrale.

3.1.3.2. Esecuzione delle attività di IT Audit

L'attività si propone l'obiettivo di pianificare ed eseguire le attività di IT audit e predisporre il rapporto finale contenente le risultanze di dettaglio dell'attività di verifica svolta.

La metodologia dell'attività di IT Audit sarà concordata con la Funzione Monitoraggio e

audit IT della DCSIT e, in conformità con gli standard di Audit già adottati (IPPF edizione 2013), dovrà basarsi sui principi di:

- indipendenza: deve essere rispettato il criterio della Segregation of duty, ovvero il personale del fornitore coinvolto nelle attività oggetto dell'IT Audit non deve essere coinvolto su ulteriori attività presso l'Amministrazione per prevenire possibili conflitti di interesse;
- imparzialità ed obiettività: il fornitore del servizio si impegna a riportare fedelmente, con obiettività ed accuratezza quanto emerso nei controlli, comprese le difficoltà incontrate e comprese eventuali opinioni divergenti emerse all'interno del team di audit;
- approccio basato sulle evidenze: tutte le attività svolte devono essere documentate per permettere la verifica di quanto emerso e per garantire l'affidabilità e riproducibilità delle conclusioni in un processo di audit sistematico.

Le sessioni di audit saranno avviate solo dopo l'approvazione da parte della DCSIT dei deliverable dell'attività di valutazione e gestione dei rischi IT e del piano di audit e saranno distribuite nel corso del periodo contrattuale(24 mesi) garantendo, per quanto possibile, un adeguato grado di regolarità delle attività senza pregiudicare, nel contempo, l'operatività della DCSIT.

Sulla base di tali criteri si prevede di sottoporre ad attività di IT Audit:

- fino a 20 (venti) processi tra quelli in perimetro, nel corso del primo anno di validità contrattuale;
- fino a 33(trentatré) processi tra quelli in perimetro, nel corso del secondo anno di validità contrattuale.

In questa fase si richiede lo svolgimento delle seguenti attività:

- la predisposizione del piano della fornitura di IT audit, per i due anni previsti dall'incarico;
- la predisposizione, ad inizio di ciascun anno contrattuale, del piano di IT audit annuale;
- la predisposizione della pianificazione puntuale delle attività previste dal piano di audit e la sua condivisione con le funzioni coinvolte;
- l'esecuzione del follow-up sui risultati di precedenti attività di IT Audit;
- la preparazione e la verifica dell'adeguatezza dei processi sottoposti ad audit con riferimento a tutte le fattispecie di rischio individuate;
- l'esecuzione delle verifiche ispettive volte al test del disegno e dell'implementazione dei controlli con relativa predisposizione di verbali a

supporto dei test svolti, corredata da evidenze opportunamente raccolte a documentazione delle attività effettuate;
- la predisposizione di documentazione a conclusione dell'audit, con la rilevazione delle criticità e delle conseguenti azioni migliorative suggerite.

Si evidenzia che questa fase dovrà essere gestita e documentata tramite strumenti proprietari, tutt'ora in corso di evoluzione, che l'Amministrazione metterà a disposizione dell'Aggiudicatario in occasione dell'incontro di avvio attività (kick-off).

DELIVERABLE ATTESI

I deliverable che dovranno essere consegnati contestualmente allo svolgimento di queste attività sono riepilogati di seguito:

- il Piano della fornitura di IT audit, per i due anni previsti dall'incarico;
- il documento del piano di IT Audit annuale, per i due anni oggetto dell'incarico e per la definizione puntuale dei test che dovranno essere effettuati;
- i verbali di IT Audit, corredati dalla documentazione opportunamente raccolta;
- al termine di ogni sessione di IT Audit, il rapporto di IT Audit riportante gli esiti delle attività effettuate, tra cui, a titolo esemplificativo e non esaustivo:
  - il perimetro dei controlli testati;
  - un Executive Summary dei risultati per la presentazione al management;
  - la valutazione dell'adeguatezza di ogni controllo verificato;
  - la descrizione di eventuali carenze di disegno dei controlli e l'indicazione delle azioni correttive da intraprendere;
  - la descrizione di un action plan, condiviso prima con l'Internal Audit e quindi con i process owner, per la risoluzione delle eventuali carenze riscontrate con indicazione dei responsabili di riferimento e delle tempistiche entro le quali colmare i gap rilevati, o l'esplicitazione di eventuali motivazioni di non accoglimento o parziale accoglimento di quanto suggerito, con valorizzazione del rischio residuo connesso.

I rapporti di IT Audit dovranno essere condivisi e validati da parte della Funzione Monitoraggio e audit IT della DCSIT. I risultati saranno condivisi e illustrati al Direttore Centrale.

3.1.3.3. Supporto specialistico per l'attività di indirizzo e coordinamento della Funzione Monitoraggio e audit IT

Le attività previste per questa fase si propongono l'obiettivo di supportare la Direzione e la Funzione Monitoraggio e audit IT nello svolgimento della propria attività istituzionale in termini di conseguimento degli obiettivi ad esso riconosciuti.

Si evidenzia che le attività per questa fase progettuale non sono definite a priori in quanto, essendo servizi specialistici che, data la loro natura, sono descrivibili in termini generici, ma non sono quantificabili ne pianificabili a priori, saranno definite al presentarsi delle singole esigenze di supporto all'indirizzo e coordinamento della Funzione Monitoraggio e audit IT.

Sarà cura della Funzione Monitoraggio e audit IT individuare i singoli "interventi" che di volta in volta si renderanno necessari e di cui darà descrizione al fornitore dal quale attenderà:

- la descrizione dell'approccio metodologico;
- la pianificazione generale con l'indicazione dell'impegno previsto per il mix di risorse proposto;
- la descrizione dei deliverable previsti.

Sarà facoltà della Funzione Monitoraggio e audit IT approvare o rifiutare la proposta di "intervento" presentata dall'impresa.

L'impresa sarà tenuta a rendere disponibili all'Amministrazione le risorse per l'esecuzione delle attività approvate entro 10 (dieci) giorni lavorativi dall'approvazione della proposta d'intervento da parte dell'Amministrazione. In caso di inadempimento da parte dell'impresa del predetto obbligo troveranno applicazione le penali contrattuali.

A titolo puramente esemplificativo e non esaustivo, possono rientrare tra le attività a richiesta:

- il supporto nella diffusione della nuova cultura all'interno dell'organizzazione tramite sessioni di training in aula, dimensionate per le diverse funzioni e ruoli aziendali;
- la predisposizione e la manutenzione del Manuale operativo della Funzione Monitoraggio e audit IT;
- la predisposizione e successiva analisi di questionari al fine di raccogliere il feedback degli utenti circa la nuova cultura aziendale;
- la manutenzione del modello di Risk Assessment e Risk Management;
- il supporto nella manutenzione del sistema di controllo interno in ambito IT;
- la predisposizione, e successiva valorizzazione, di indicatori volti a valutare l'efficacia dell'attività della Funzione Monitoraggio e audit IT in un'ottica di

miglioramento continuo del processo di IT internal auditing.

Una volte eseguita l'attività approvata dall'Amministrazione, l'Impresa dovrà consegnare un consuntivo che riporti il numero delle giornate erogate per ciascuna risorsa professionale; tale documento sarà condiviso e validato da parte della Funzione Monitoraggio e audit IT della DCSIT.
Il numero delle giornate effettivamente erogate non potrà essere superiore a quanto riportato nella proposta approvata, con un limite di aumento del 10%.

DELIVERABLE ATTESI

I deliverable attesi saranno di volta in volta concordati con la Funzione Monitoraggio e audit IT, sulla base della tipologia di supporto richiesta.

3.1.4. Durata della fornitura – Lotto 1

Le attività previste nel Lotto 1 dovranno concludersi entro il termine massimo di 24 mesi dalla "data di avvio della fornitura", come definita nel successivo capitolo 5.

Il piano di lavoro della fornitura dovrà essere presentato dall'Aggiudicatario in fase di avvio della fornitura e sarà sottoposto all'approvazione della Funzione Monitoraggio e audit IT.

3.1.5. Deliverable della fornitura – Lotto 1

Nel presente paragrafo si riassumono i deliverable previsti dalla fornitura, fermo restando che DCSIT si riserva di modificare formalismo e contenuti durante il corso della fornitura stessa.

Tutti i documenti dovranno essere particolarmente curati negli aspetti di:

- comprensibilità;
- accuratezza;
- adeguatezza;
- aderenza;
- modificabilità.

Tutta la documentazione dovrà essere prodotta sia su supporto elettronico che cartaceo, ove richiesto dall' Amministrazione, e consegnata anche nel formato sorgente dei singoli tools utilizzati (ad esempio Excel).

Tutti i prodotti consegnati sono soggetti ad approvazione da parte della Funzione

Monitoraggio e audit IT; in nessun caso l'approvazione potrà avvenire per tacito assenso.

I deliverable previsti per il Lotto 1 sono elencati in

Tabella **2**, unitamente ai relativi livelli di servizio attesi ed Indici di Qualità (IQ).

Evento/Servizio	Deliverable	IQ	Livelli di Servizio
Avvio della fornitura	Piano di lavoro della fornitura	IQ05	Entro 15 (quindici) giorni lavorativi dalla stipula del contratto. Entro 5 (cinque) giorni lavorativi dalla fine del semestre di riferimento per i successivi aggiornamenti
	Piano della Qualità Generale	IQ05	Entro 15 (quindici) giorni lavorativi dalla stipula del contratto.
Riunione di Kick Off della fornitura	Presentazione a supporto della riunione di Kick Off della fornitura	IQ05	Entro 15 (quindici) giorni lavorativi dalla stipula del contratto.
Riunione di Stato Avanzamento Lavori	Documento di Stato Avanzamento Lavori	IQ05 IQ06	Secondo le cadenze concordate con il referente dell'Amministrazione all'avvio della fornitura e riportate nel piano di lavoro del servizio.
Al termine di ciascun servizio	Presentazione dei risultati per il management	IQ05	Secondo le tempistiche previste dal piano di lavoro del servizio.
Valutazione e gestione dei rischi IT	Piano di lavoro del servizio	IQ05	Entro 5 (cinque) giorni lavorativi dall'avvio del servizio. Entro 5 (cinque) giorni lavorativi dalla richiesta di aggiornamento da parte dell'Amministrazione o dal SAL, per i successivi aggiornamenti.

Evento/Servizio	Deliverable	IQ	Livelli di Servizio
	Mappatura processi IT in perimetro	IQ05 IQ06	Secondo le tempistiche previste dal piano di lavoro del servizio.
	Verbali delle interviste con i process owner		
	Questionari di rilevazione compilati dai process owner		
	Risk Control Matrix		
	Executive Summary		
	Technical Report		
	Action Plan		
Esecuzione delle attività di IT Audit	Piano della fornitura di IT audit	IQ05	Entro 10 (dieci) giorni lavorativi dalla conclusione del servizio di Valutazione e gestione dei rischi IT (con l'approvazione di tutti i deliverable previsti).
	Piano di IT Audit annuale	IQ05	Entro 10 (dieci) giorni lavorativi dalla predisposizione del Piano della fornitura di IT audit, per il primo anno contrattuale. Entro 10 (dieci) giorni lavorativi dall'inizio del secondo anno contrattuale, per il secondo anno contrattuale.
	Verbali di IT Audit	IQ05 IQ06	Secondo le tempistiche previste dal Piano di IT Audit annuale.
	Rapporto di IT Audit	IQ05 IQ06	Entro 10 (dieci) giorni lavorativi dalla chiusura della singola sessione di IT Audit prevista dal piano di IT Audit annuale.
Supporto specialistico per l'attività di	Piano di lavoro del servizio	IQ05	Entro 5 (cinque) giorni lavorativi dalla richiesta di supporto.

Evento/Servizio	Deliverable	IQ	Livelli di Servizio
indirizzo e coordinamento della Funzione Monitoraggio e audit IT	Deliverable concordati con la Funzione Monitoraggio e audit IT sulla base della tipologia di supporto richiesta	IQ05 IQ06	Secondo le tempistiche previste dal piano di lavoro del servizio.
Per ogni servizio	Rapporto indicatori di qualità	IQ05	Entro 5 (cinque) giorni lavorativi dall'inizio del mese successivo al trimestre di rilevazione.

Tabella 2– Deliverable previsti per il Lotto 1

Nel corso delle attività, potranno essere individuate altre tipologie di deliverable da consegnare i cui contenuti saranno congiuntamente concordati.

3.1.6. Gruppo di lavoro e profili professionali – Lotto 1

Il Fornitore, nell'elaborazione della sua offerta, dovrà dare una descrizione dettagliata della struttura organizzativa del progetto.

L'esecuzione delle attività di "Valutazione e gestione dei rischi IT" si prevede un unico intervento progettuale.

Per l'esecuzione delle attività di "IT Audit" saranno definite "sessioni di audit" per le quali si prevede un massimale in Giorni Persona (GP), quale somma delle dimensioni in giorni persona delle singole "sessioni di audit", il cui corrispettivo è calcolato sulla base dei GP della sessione di IT Audit e del costo risultante dalla media ponderata delle figure professionali e della percentuale di utilizzo prevista per il servizio in oggetto.

Il massimale di impegno previsto per l'esecuzione delle attività di IT Audit è di 394 GP.

Relativamente alla composizione del gruppo di lavoro, questa dovrà garantire, per ciascun servizio, almeno il mix di riferimento riportato in

Tabella **3**.

Figura professionale	Servizio

	Valutazione e gestione rischi IT (Impegno %)	Esecuzione delle Attività di IT Audit (Impegno %)
Manager	35 %	12 %
Consulente Senior	45 %	56 %
Consulente Junior	20 %	32 %

Tabella 3 - Mix di impegno per figura professionale e servizio

I mix riportati nella tabella precedente sono quelli ritenuti ottimali dalla Committente, tuttavia il fornitore può 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. Eventuali scostamenti dovranno essere preventivamente comunicati e motivati dal Fornitore in fase di pianificazione eaccettati dal referente della Committente. In tal caso il corrispettivo riconosciuto al fornitore è calcolato sulla base del prezzo unitario offerto per singola figura professionale.

Relativamente ai servizi di Indirizzo e coordinamento per la funzione di Monitoraggio e audit IT, l'Amministrazione prevede di fruire di complessive 270 giornate uomo, ripartite sulle figure professionali previste (cfr. paragrafo 3.1.6) come da

Tabella **4**.

Figura professionale	Giorni per figura professionale
Manager	94
Consulente Senior	136
Consulente Junior	40

Tabella 4 - Previsione d'impegno per i servizi di indirizzamento e coordinamento

Si precisa che tali quantità sono da ritenersi puramente indicative ed in alcun modo vincolanti per l'Amministrazione, che potrà richiedere un quantitativo inferiore rispetto a quello stimato o diversamente ripartito tra le sopra indicate figure professionali.

***

Si richiede che il gruppo di lavoro, che l'impresa proporrà per lo svolgimento dei servizi oggetto della fornitura, soddisfi i profili di seguito descritti. I curriculum vitae del personale da impiegare nei vari servizi dovranno essere resi disponibili all'Amministrazione secondo quanto previsto nelle condizioni speciali dello schema di contratto. L'Amministrazione si riserva di indicare un template per la raccolta dei curriculum vitae del personale impiegato nella fornitura. Per quanto attiene alle risorse che possiedono le certificazioni eventualmente offerte, si precisa che queste dovranno essere rese disponibili per l'intera efficacia del contratto e dovranno essere impiegate nei gruppi di lavoro che garantiscono l'erogazione dei servizi oggetto della fornitura anche senza espressa richiesta dell'Amministrazione.

L'Impresa dovrà consegnare unitamente ai curricula ed alle eventuali certificazioni documentazione atta a dimostrare il rapporto di lavoro del personale impiegato nell'appalto, alla luce di quanto dichiarato in offerta tecnica.

Manager

Profilo

Laureato con anzianità lavorativa maggiore di 10(dieci) anni, da computarsi successivamente alla data di conseguimento del diploma di laurea, di cui almeno 3 (tre) 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 comprovata di project management in progetti analoghi;
- conoscenza delle metodologie di Risk Assessment;
- conoscenza dei processi di IT Governance e IT Management;
- esperienza comprovata nel disegno e nella valutazione dei sistemi di controllo interno;
- conoscenza delle metodologie e degli strumenti operativi richiesti in progetti di IT Audit;
- conoscenza dei processi e delle procedure operative IT;
- certificazione CISA;
- competenza ed esperienza comprovata nelle metodologie di Internal Audit IT secondo gli standard citati.

Consulente senior

Profilo

Laureato con anzianità lavorativa di almeno 7 (sette) anni, da computarsi successivamente alla data di conseguimento del diploma di laurea, di cui almeno 3(tre) anni di comprovata 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 delle metodologie e degli strumenti di Risk Assessment;
- conoscenze approfondite delle tecniche di Risk Management;
- esperienza comprovata nella conduzione di Risk Assessment;
- conoscenza complessiva delle problematiche di sicurezza dei dati e delle Informazioni;
- certificazione CISA;
- conoscenza delle metodologie e delle tecniche di IT Audit;
- conoscenza dei sistemi di controllo in ambito IT;
- conoscenza dei processi e delle procedure operative IT;
- esperienza comprovata nella conduzione di IT Audit.

Consulente junior

Profilo

Laureato con anzianità lavorativa di almeno 3 (tre) 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:

- conoscenza delle tecniche e delle metodologie di Risk Assessment;
- partecipazione comprovata a progetti di Risk Assessment;
- conoscenza delle tecniche e delle metodologie di IT Audit;
- partecipazione comprovata a progetti di IT Audit.

3.2. Lotto 2: Controllo dell'efficacia delle misure di sicurezza IT

3.2.1. Contesto di riferimento – Lotto 2

Alla Funzione Sicurezza, sono riconosciute in sintesi le seguenti responsabilità:

- definizione della strategia e dei principi da applicare per abbattere il rischio informatico e per pianificare l'evoluzione del SGSI, uniformandolo, laddove necessario, alla normativa vigente e agli standard internazionali;
- emissione di Politiche di sicurezza che descrivono le modalità di attuazione delle strategie di sicurezza con un dettaglio sufficiente a renderle attuabili;
- definizione e gestione del piano di continuità dei servizi IT;
- prevenzione degli incidenti di sicurezza.

A valle di tali compiti, nel pieno rispetto del paradigma Plan, do, Check, Act, nasce l'esigenza di implementare le attività tipiche della fase di Check, secondo la logica che tutti i compiti connessi siano affidati ad un soggetto terzo ed indipendente, ovvero non affidati allo stesso personale che ha svolto attività operative (ad.es. configurazione, implementazione sistemi e applicazioni …) per INAIL. Tali compiti si possono riassumere in:

- verificare l'effettiva e corretta attuazione degli standard di Sicurezza definiti dalla Direzione e la conformità alle normative;
- verificare l'efficacia del sistema di sicurezza in essere.

Il fornitore nel formulare la sua offerta deve tenere in considerazione che l'Amministrazione dispone di:

- 30 linee guida/ best practice di sicurezza informatica;
- sistema interno dei controlli in ambito sicurezza, riportante le corrispondenti attività di controllo poste in essere ai fini della conformità al Decreto Legislativo 196/2003 ed in particolare all'Allegato B e ai Provvedimenti del garante applicabili a INAIL, al D.Lgs 231/2001;
- Geco, strumento software proprietario per l'esecuzione di campagne di verifica della conformità;
- suite McAfee Vulnerability Manager;
- suite ArcSight;
- Compliance Pack di ArcSight;
- McAfee Policy auditor;
- McAfee Risk Advisor.

3.2.2. Perimetro della fornitura – Lotto 2

Infrastruttura Informatica

L'infrastruttura informatica dell'Amministrazione è gestita dallo staff tecnico della DCSIT e consta di un accesso ad Internet ridondato , 1200 reti LAN, circa 1000 server , 10000

postazioni client e 250 collegamenti con fornitori di servizi, di cui 240 relativi ai collegamenti geografici delle sedi periferiche, e 10 collegamenti sulle sedi della Business continuity a livello centrale.

Le sale server presenti presso le sedi di Ferruzzi e di Tiburtino sono gemelle ed ospitano ciascuna 298 server tra cui 1 mainframe, 1 Power 7 e 2 superdome. Le due sedi ospitano, inoltre, l'infrastruttura di networking per l'accesso ad Internet ed alle altre reti di fornitori esterni.

I client dell'Amministrazione sono su piattaforma Microsoft Windows 7 e la maggior parte dei server dipartimentali sono su piattaforma Microsoft Windows 2003 e 2008 Server.

La rete geografica delle sedi periferiche (collegamenti da 2 a 10 Mbs su tecnologia MPLS) e quella delle sedi centrali (collegamenti da 200 Mb a 1Gb) sono gestite in outsourcing dal fornitore della connettività.

La connessione ad Internet ridondata è in fibra ottica (5 Gbps), con 4 reti pubbliche per un totale di 256 indirizzi IP e viene utilizzata, oltre che per la navigazione e gli altri accessi ad Internet, per la messaggistica e l'accesso remoto in VPN.

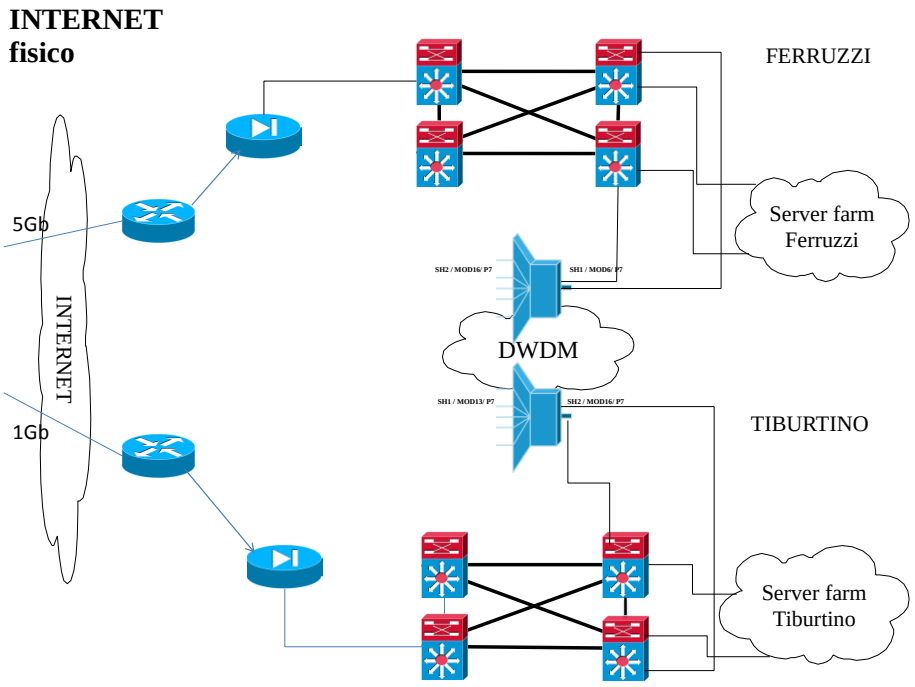
Il perimetro di intervento per le attività di analisi delle vulnerabilità si può riassumere, per ogni anno contrattuale, in:

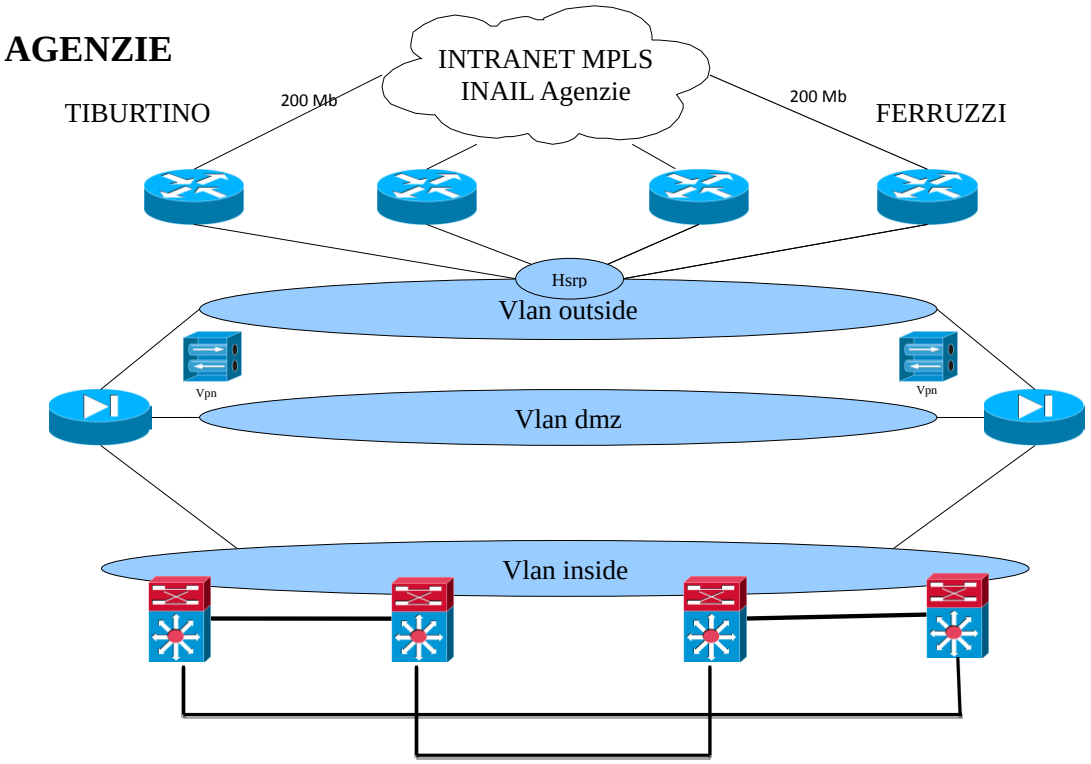
- 370 applicazioni, di cui 35 esposte su Internet;
- circa 5000 indirizzi IP;
- server di posta elettronica;
- infrastruttura di sicurezza e networking;
- apparecchiature per la gestione complessiva della rete.

Il perimetro di intervento per le attività di penetration test si può riassumere, per ogni anno di validità contrattuale, in:

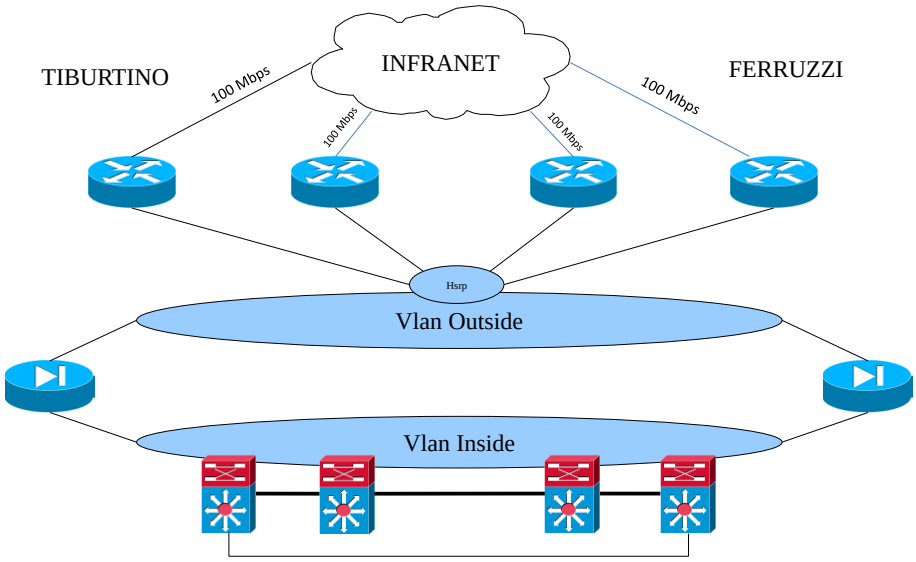
- 35 applicazioni esposte su Internet, per le attività di PT su applicazioni web raggiungibili pubblicamente attraverso Internet;
- 85 applicazioni interne, per le attività di PT su applicazioni presenti sulle reti private.

Di seguito si inseriscono i diagrammi di rete delle varie connettività:


INTERNET
fisico
FERRUZZI
5Gb
INTERNET
1Gb
Server farm
Ferruzzi
DWDM
TIBURTINO
Server farm
Tiburtino


AGENZIE
INTRANET MPLS
INAIL Agenzie
TIBURTINO
200 Mb
200 Mb
FERRUZZI
Hsrp
Vlan outside
Vpn
Vpn
Vlan dmz
Vlan inside

INFRANET


TIBURTINO
INFRANET
FERRUZZI
100 Mbps
100 Mbps
100 Mbps
100 Mbps
Hsrp
Vlan Outside
Vlan Inside

3.2.3. Oggetto della fornitura – Lotto 2

Oggetto della fornitura del presente Lotto è il supporto tecnico-metodologico alle attività di verifica sullo stato della sicurezza dei sistemi informativi dell'INAIL. In particolare, la DCSIT intende affidare all'aggiudicatario i seguenti servizi, dettagliati nei paragrafi a seguire:

3.2.3.1. IT Security Audit, per verificare l'effettiva attuazione del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) definito dalla Funzione Sicurezza;
3.2.3.2. Analisi delle attività degli Amministratori di Sistema, in conformità al Provvedimento del Garante per la Privacy;
3.2.3.3. ICT Security Assessment, per valutare il livello di sicurezza dei sistemi, delle componenti infrastrutturali, della rete e delle componenti di security in essere (firewall, IDS/IPS, SSO, Proxy, sistemi di log, etc.).

A seguito dell'assegnazione delle attività il fornitore dovrà predisporre un piano di lavoro della fornitura, in accordo con la Funzione Sicurezza, che ne potrà chiedere la rimodulazione, comprendente le attività di controllo previste. Il piano di lavoro della fornitura dovrà prevedere la distribuzione delle attività di analisi nel corso di ogni anno contrattuale garantendo, per quanto possibile, un adeguato grado di regolarità delle attività senza pregiudicare, nel contempo, l'operatività della DCSIT. Il piano di lavoro della fornitura dovrà, inoltre, essere predisposto in modo tale da organizzare l'insieme dei servizi secondo un ordine di priorità che tenga conto:

- delle esigenze strategiche ed operative dell'Amministrazione;
- delle aree di attività che risultano maggiormente critiche sulla base dell'attuale situazione e delle esigenze future (evoluzioni tecnologiche, possibili cambiamenti operativi, ecc.);
- della necessità di articolare le varie attività di sicurezza secondo criteri di efficienza e di creazione di possibili sinergie.

Si precisa che è richiesta all'Aggiudicatario la predisposizione, secondo le tempistiche riportate in

Tabella **6** e in coerenza con il piano di lavoro della fornitura, del piano di lavoro per il singolo servizio richiesto (piano di lavoro del servizio) che dovrà essere condiviso ed approvato dalla Funzione Sicurezza.

Con riferimento al singolo servizio è previsto che l'Amministrazione ne comunichi formalmente l'avvio.

3.2.3.1. IT Security Audit

L'aggiudicatario sarà tenuto a controllare, con frequenza semestrale, l'effettiva attuazione delle policy, delle linee guida e degli standard di sicurezza definiti dalla Funzione Sicurezza e a verificare la conformità alle normative e alle best practice e standard di riferimento, tra cui i benchmarks CIS e lo standard ISO/IEC 27001.

Relativamente alla conformità alle normative vigenti sulla specifica tematica, l'Aggiudicatario dovrà verificare che il SGSI in essere ed il relativo sistema di controllo interno indirizzino correttamente e pienamente i requisiti di sicurezza previsti dalle normative, quali a titolo esemplificativo ma non esaustivo:

- Decreto Legislativo n° 196/2003 - Codice in materia di protezione dei dati personali, e successive modificazioni, integrazioni e Provvedimenti applicabili al contesto di INAIL;
- Decreto Legislativo n° 231/2001 - Disciplina della responsabilità Amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300, relativamente agli articoli introdotti con la Legge 48/2008 che inseriscono i reati informatici fra quelli presupposti dal decreto;
- Decreto Legislativo n° 82/2005 - Codice dell'Amministrazione Digitale, e successive modificazioni ed integrazioni.

Il fornitore dovrà predisporre la verifica definendo l'opportuna mappatura tra requisiti di controllo e asset da controllare. Durante la campagna dovrà supportare l'esecuzione dei controlli di verifica effettuando, all'occorrenza, interviste sulla base di questionari già predisposti. In presenza di evoluzioni normative e/o variazioni del perimetro di asset da sottoporre a verifica, il fornitore dovrà procedere all'opportuna revisione dei controlli.

L'analisi dovrà prevedere, in prima istanza, l'esecuzione di un'attività di follow-up sulle azioni individuate in esito alla precedente campagna di controllo al fine di identificare eventuali criticità nell'attuazione delle azioni correttive pianificate e di rilevare lo stato dell'arte dei controlli in essere.

Nella formulazione della sua offerta, il fornitore dovrà considerare che la Funzione Sicurezza metterà a sua disposizione, dalla data di inizio delle attività, i seguenti strumenti di supporto alle attività di verifica:

- Geco, prodotto software personalizzato per INAIL, che consente di automatizzare campagne di verifica della conformità sia mediante controlli automatizzati, sia mediante questionari. In particolare l'esecuzione dei controlli automatici di Geco avviene mediante l'utilizzo di adapter verso sorgenti informative (es. sistemi

operativi, database) o piattaforme già presenti nell'Amministrazione, quali McAfee Vulnerability Manager e ArcSight. Geco consente la definizione di apposite campagne di verifica per l'esecuzione automatica dei controlli e la raccolta dei dati previsti dai questionari. L'utilizzo di Geco non richiede competenze specialistiche a livello tecnologico mentre è richiesta la competenza funzionale nell'esecuzione di Audit e nell'utilizzo di soluzioni di GRC.

- Compliance Pack di ArcSight;
- McAfee Policy auditor;
- McAfee Risk Advisor.

DELIVERABLE ATTESI

Al termine della campagna di verifica il Fornitore dovrà produrre:

- un Executive Summary, contenente la sintesi dei risultati delle attività di verifica e dell'attività di follow-up;
- un Technical Report, contenente il dettaglio degli esiti della campagna di verifica, tra cui evidenza delle eventuali esigenze di rientro dalle non conformità e lo scostamento rispetto alle verifiche precedenti;
- un Remediation Plan, riportante, ad alto livello, l'indicazione delle attività da porre in essere per risolvere le non conformità rilevate e la relativa priorità di implementazione.

3.2.3.2. Analisi delle attività degli Amministratori di Sistema

L'attività richiesta si pone l'obiettivo di effettuare, con frequenza annuale, le verifiche sull'operato degli amministratori di sistema in conformità allo specifico obbligo richiesto dal Garante della Privacy con il Provvedimento del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema (G.U. n. 300 del 24-12-2008)".

La verifica dovrà essere effettuata con cadenza annuale e dovrà essere incentrata sulla rispondenza dell'operato degli amministratori di sistema alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dal suddetto Provvedimento.

I controlli per la verifica dell'operato degli Amministratori di Sistema dovranno essere commisurati alla criticità dei dati e differenziati per tipologia di dati personali, con maggior livello di dettaglio relativamente ai dati sensibili o giudiziari.

Nella formulazione dell'approccio metodologico per l'esecuzione dell'attività, il fornitore

deve tenere in considerazione che sarà messa a sua disposizione la suite ArcSight, attraverso la quale potrà effettuare le ricerche e produrre i report utili ai fini delle attività di analisi dei log dei sistemi e, in particolare, dei dati di login e logout degli Amministratori di Sistema. La

Tabella **5** elenca le appliance e le componenti della suite ArcSight attualmente in essere presso l'Amministrazione.

Si precisa che le appliance C5100 e 7100X,tutte in End Of Life e End Of Support, saranno oggetto, nel corso del 2014,del progetto "RefreshArcSight" che porterà alla loro sostituzione con, rispettivamente, 8 appliance C5500 e 2 appliance L7500X

Modello	Tipologia	Quantità	Versione software attuale
C5100	Connector Appliance	20	6.3-C6386
C5400	Connector Appliance	1	6.4-C6661
L7100X	Logger Appliance	2	5.3 SP1-L6838
L7400-SAN	Logger SAN Appliance	2	5.3 SP1-L6838
M7200XL	Correlatore	2	5.0.1.6642.2 (5.0 SP1 Patch 2)
B7400	Correlatore	1	5.1.0.1281.3 (ESM Express 3.0)

Tabella 5 - Suite ArcSight

DELIVERABLE ATTESI

I deliverable che dovranno essere consegnati contestualmente allo svolgimento delle attività illustrate sono riepilogati di seguito:

- metodologia di audit dei log degli amministratori di sistema;
- Executive Summary, riportante la sintesi dei risultati dell'attività di analisi;
- Technical Report, riportante il dettaglio dei risultati dell'analisi, tra cui, a titolo esemplificativo e non esaustivo, gli accessi anomali rilevati, i rischi riscontrati;
- Remediation Plan, riportante l'indicazione, ad alto livello, delle possibili contromisure tecnologiche e/o organizzative da porre in essere per eliminare le cause di non conformità rilevate e la relativa priorità di implementazione.

3.2.3.3. ICT Security Assessment

L'analisi è mirata alla revisione delle misure di sicurezza implementate a livello logico e fisico 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 falle nei sistemi operativi e nelle applicazioni installate e loro configurazioni 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.

Il piano temporale di dettaglio per tutte le attività di analisi, ovvero il piano di lavoro del servizio, dovrà essere concordato con la Funzione Sicurezza e da esso approvato.

Le attività di analisi potranno essere svolte durante le giornate feriali: da lunedì a venerdì, dalle 08:30 alle 17:30.

I test saranno eseguiti su sistemi e reti in esercizio; le attività che potrebbero causare blocchi o disservizi dovranno essere preventivamente concordate e pianificate e dovranno tenersi tra le 18:30 e le 22:00 (oppure nella giornata di sabato/domenica).

Il personale di DCSIT potrà partecipare alle attività effettuate nell'ambito dell'erogazione dei servizi di Vulnerability Assessment e Penetration Test in qualità di osservatore.

Durante le attività sarà a disposizione dell'Aggiudicatario un tecnico dello staff di DCSIT per fornire tutte le informazioni tecniche e logistiche necessarie per una corretta e sicura esecuzione dei test e delle verifiche.

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 responsabili dello staff tecnico di DCSIT in caso di problemi o disservizi.

I dati che saranno rilevati durante l'analisi ed in qualsiasi altra fase dell'elaborazione dovranno essere conservati con la massima cura; acquisiti e conservati solamente se

strettamente necessari all'elaborazione, e dovranno essere distrutti in maniera sicura (o riconsegnati) dopo la produzione dei deliverable.

Prima dell'inizio delle attività, il fornitore dovrà sottoscrivere un accordo di riservatezza che lo impegna a non divulgare nessuna informazione relativa a INAIL, alle sue infrastrutture informatiche ed ai suoi dati.

La documentazione prodotta a presentazione dei risultati dovrà essere in lingua italiana, ad eccezione dei contenuti dei report generati in automatico dagli strumenti che il fornitore intenderà utilizzare a supporto delle attività di vulnerability assessment (VA) e penetration test (PT), che potranno essere in lingua inglese.

L'ICT Security Assessment dovrà prevedere le seguenti attività:

3.2.3.3.1. VA e PT su sistemi e applicazioni web raggiungibili pubblicamente attraverso Internet;

3.2.3.3.2. VA e PT sui sistemi e applicazioni presenti sulle reti private;

3.2.3.3.3. Analisi delle misure di sicurezza infrastrutturali.

Si precisa che l'Aggiudicatario dovrà, con le frequenze di seguito indicate, pianificare ed effettuare le analisi sul parco applicativo in perimetro, ossia sull'insieme di applicazioni in esercizio. Con la stessa modalità dovrà essere verificata la sicurezza delle infrastrutture presenti nell'Amministrazione e di quelle eventualmente acquisite nel corso del periodo di validità del contratto.

3.2.3.3.1. VA e PT su sistemi e applicazioni web raggiungibili pubblicamente attraverso Internet

Scopo dell'intervento è verificare, con frequenza semestrale, il livello di rischio nei confronti di attacchi portati attraverso la connessione ad Internet dell'Amministrazione, sia verso i server che espongono pubblicamente servizi, che verso la rete interna, identificando eventuali vulnerabilità che consentano di ottenere un accesso remoto non autorizzato all'infrastruttura informatica e/o ai dati in essa contenuti.

Si vuole, in particolare, verificare la resistenza agli attacchi dei sistemi e dei 35 applicativi esposti pubblicamente su **web e mobile** e delle difese perimetrali nel loro complesso, determinando la possibilità di sfruttare falle nel sistema operativo e negli applicativi installati e loro configurazioni con finalità di accesso non autorizzato, privilege escalation, furto di informazioni, atti di vandalismo, manomissione e interruzione dei servizi erogati.

L'analisi dovrà essere condotta direttamente attraverso Internet, con modalità "black box", ovvero senza conoscenza pregressa dell'infrastruttura e delle configurazioni, senza accesso fisico ai sistemi e senza credenziali di accesso, simulando il comportamento di un attaccante reale.

Le attività minime richieste sono:

- mappatura di tutti i servizi pubblicamente raggiungibili sugli indirizzi oggetto dell'analisi, identificazione delle politiche di routing e filtro, identificazione di sistemi operativi, software, versioni e configurazioni coinvolte ed altre informazioni potenzialmente utili per un attaccante;
- verifica dello stato di sicurezza (vulnerabilità, patch level, configurazioni, etc.) dei servizi e dei software raggiungibili ed identificazione di eventuali punti deboli in sistemi, software ed applicazioni nonché nell'infrastruttura di rete e di difesa perimetrale;
- identificazione di eventuali utenze con credenziali (username/password) facilmente deducibili, risorse non pubblicamente disponibili (url "nascosti", etc.) ed altre informazioni utili ai fini di un attacco;
- compatibilmente con il livello di rischio di disservizio per un'infrastruttura in produzione:
    - effettuare una simulazione di attacco mirata ad accedere a dati normalmente non raggiungibili;
    - sovvertire il normale funzionamento delle applicazioni;
    - eseguire codice arbitrario.
- verifica della possibilità di usare i sistemi compromessi come testa di ponte per attaccare verso altri sistemi presenti nella stessa zona di rete, verso Internet e verso altre zone di rete
- identificazione del root-cause delle vulnerabilità rilevate;
- identificazione e pianificazione degli interventi di remediation da porre in essere per contrastare le vulnerabilità rilevate.

La metodologia di assessment proposta dal fornitore per l'esecuzione delle attività richieste dovrà integrare standard internazionali quali NIST-SP800-115 e OSSTMM, al fine di garantire l'implementazione delle seguenti fasi operative:

- Footprinting: raccolta delle informazioni da canali ad accesso pubblico o mediante interrogazione dei servizi pubblicamente accessibili;
- Network Discovery: identificazione dei servizi accessibili nei sistemi. Particolare attenzione dovrà esser posta nell'identificazione dei servizi e dei sistemi operativi pubblicamente accessibili;
- VulnerabilityScan: identificazione e verifica delle vulnerabilità dei sistemi sotto analisi;
- Operational *Security*: analisi sui sistemi di produzione delle vulnerabilità e sfruttamento delle stesse (Penetration Test) per ottenere maggiore accesso ai sistemi.

In particolare, la fase di Operational Security vuole verificare, in relazione allo stato attuale della tecnologia ed alle metodologie di attacco pubblicamente conosciute, la possibilità di sfruttare falle nei sistemi operativi e nelle applicazioni installate e loro configurazioni al fine di accedere illegalmente, rubare o manomettere informazioni, commettere atti di vandalismo, interrompere i servizi erogati, etc.. L'analisi dovrà avvenire tramite verifiche dirette incentrate principalmente sugli argomenti elencati, a titolo esemplificativo e non esaustivo, qui di seguito:

- Validazione dei dati di input (validazione client-side, cross-site scripting, comandi diretti al sistema operativo, comandi SQL diretti al DBMS, attraversamento di percorsi, metacaratteri, caratteri nulli);
- Trasformazioni canoniche (Case sensitivity, codifica Unicode, codifica UTF, problematiche specifiche del file system e del sistema operativo, trattamento delle estensioni dei file, trattamento della codifica MIME);
- Manipolazione di parametri (manipolazione dei cookie, manipolazione dei campi di input, manipolazione di header HTTP, manipolazione dell'URL);
- Autenticazione e session management (attacchi brute force, Infrastructure authentication, Session Hijacking, Session Replay);
- Configuration Management (password indovinabili, mancati aggiornamenti, API ed altri servizi accessibili);
- Crittografia (Keyspace, chosenPlaintext, knownCiphertext, generazione dei numeri casuali, algoritmi deboli);
- Overflow (Heap Overflow, Stack Overflow, Format Strings);
- Informazioni riservate e privacy (commenti client-side, comandi di debug, messaggi e codici di errore, enumerazione di file e di servizi, protezione della cache e della cronistoria).

Si evidenzia che al fornitore è richiesta anche un'attività di follow-up sulle azioni correttive previste in esito ad una precedente sessione di Vulnerability Assessment e Penetration Test.

Il fornitore, nella sua Offerta Tecnica, dovrà illustrare con adeguato livello di dettaglio la metodologia e gli strumenti a supporto che intenderà utilizzare per l'esecuzione delle attività richieste.

DELIVERABLE ATTESI

I deliverable attesi in esito alle attività richieste sono riepilogati di seguito:

- Executive Summary, dovrà contenere i risultati più significativi dell'analisi complessiva, quali, a titolo esemplificativo e non esaustivo: il livello di rischio e di immagine, danni potenziali, facilità e reali rischi di sfruttamento delle vulnerabilità da parte di un malintenzionato, rischi legali, soluzioni gestionali e tecniche da intraprendere per ridurre il rischio, etc.. L'Executive Summary dovrà fornire anche indicazioni sulle modalità di risoluzione delle problematiche identificate, sempre utilizzando un linguaggio business e non tecnico;

- Technical Report (uno o più documenti), dovrà contenere i dettagli tecnici particolareggiati con tutti i risultati emersi: le informazioni su tutte le vulnerabilità e problematiche di sicurezza identificate in ordine di importanza; le informazioni ed i consigli per affrontarle, nonché valutazioni sul livello reale di rischio. Questi risultati saranno oggetto di presentazione, con eventuali diapositive accompagnatorie, direttamente allo staff tecnico della DCSIT. Il documento potrà contenere termini e linguaggio specialistici, dovrà essere tuttavia di facile comprensione per lo staff tecnico, contenere una descrizione discorsiva e chiara della problematica e dell'impatto, nonché i riferimenti a documentazione ed approfondimenti (CVE o equivalenti, bollettini di sicurezza, documentazione pubblica); dove applicabile, dovranno sempre essere incluse delle dimostrazioni delle problematiche (screen shot, output di comandi, file/dati, etc.) e le procedure seguite per conseguirle (url, attacchi od exploit, etc.);

- Remediation Plan, riportante, a titolo esemplificativo e non esaustivo, l'indicazione, per ciascuna vulnerabilità individuata, della root-cause, degli interventi da porre in essere per la sua rimozione, ordinati per priorità, della stima temporale dell'intervento, della stima dell'impatto economico, organizzativo e tecnologico dell'intervento.

3.2.3.3.2. VA e PT su sistemi e applicazioni presenti sulle reti private

Scopo dell'intervento è verificare, con frequenza semestrale, il livello di rischio nei confronti di attacchi portati attraverso la rete privata o la rete geografica di INAIL, sia verso i server interni, che verso stazioni client ed altre apparecchiature (networking, stampa, telefonia, ...) identificando eventuali vulnerabilità che consentano di ottenere un accesso non autorizzato all'infrastruttura informatica e/o ai dati in essa contenuti.

Si vuole in particolare verificare la resistenza agli attacchi dei sistemi, delle applicazioni presenti sulla rete privata e dell'infrastruttura di rete geografica nel suo complesso,

determinando la possibilità di sfruttare falle nel sistema operativo e negli applicativi installati e loro configurazioni con finalità di accesso non autorizzato, privilege escalation, furto di informazioni, atti di vandalismo, manomissione e interruzione dei servizi erogati.

L'analisi dovrà essere condotta in modalità “white box” presso la sede dell’INAIL, attraverso un accesso posizionato sulla rete privata.

Si evidenzia che il fornitore non dovrà prevedere spostamenti su più sedi per l’esecuzione dell’analisi in quanto tutte le subnet interessate dalle attività di Vulnerability Assessment e Penetration Test saranno raggiungibili dal suddetto punto di accesso posizionato sulla rete privata.

Si precisa che dovranno essere sottoposte a VulnerabilityAssessment le reti wirede le reti wireless presenti nella sede centrale dell’ INAIL.

Le attività di Vulnerability Assessment minime richieste sono:

- mappatura di tutti i servizi raggiungibili sugli indirizzi oggetto dell’analisi;
- identificazione delle politiche di routing e filtro sulla rete geografica (accesso verso le filiali/Agenzie, accesso verso Internet, etc.);
- verifica dello stato di sicurezza (vulnerabilità, patch level, configurazioni, etc.) dei servizi e dei software raggiungibili ed identificazione di eventuali punti deboli in sistemi, software ed applicazioni nonché nell'infrastruttura di rete geografica;
- identificazione di eventuali utenze con credenziali (username/password) facilmente deducibili ed altre informazioni utili ai fini di un attacco;
- analisi a campione del traffico di rete per verificare quali credenziali ed informazioni siano trasmesse in chiaro e che attacchi si possano portare per sovvertire a proprio vantaggio (analisi, modifica, interruzione) il normale traffico di rete;
- identificazione delle root-cause delle vulnerabilità rilevate;
- identificazione e pianificazione degli interventi di remediation da porre in essere per eliminare le problematiche rilevate.

Relativamente al Penetration Test, è richiesta l’esecuzione delle seguenti attività minime:

- Penetration Test sulle retiwired private,al fine di evidenziare la possibilità di introdursi nella rete privata o nella rete geografica di INAIL mediante test empirici che simulano attacchi alla rete tramite l’impiego di tools automatici e/o procedure manuali in grado di sfruttare le vulnerabilità rilevate dal VA;
- Penetration Test applicativi, con la finalità di evidenziare la possibilità diintrodursi nelle applicazioni ad uso interno INAIL (sia client-server, sia prive di interfaccia utente) mediante test empirici, che simulano attacchi alle applicazioni tramite

l'impiego di tools automatici e/o procedure manuali in grado di sfruttare le vulnerabilità dell'applicazione. Compatibilmente con il livello di rischio di disservizio per un'applicazione in produzione i test saranno mirati, a titolo indicativo e non esaustivo, a:

- accedere a dati e informazioni normalmente non raggiungibili;
- sovvertire il normale funzionamento dell'applicazione;
- eseguire codice arbitrario;
- utilizzare il sistema che ospita l'applicazione come testa di ponte per attaccare altri sistemi e/o applicazioni presenti nella stessa zona di rete, verso Internet e verso altre zone di rete.

- Penetration Test su reti Wireless, finalizzato all'identificazione delle possibili azioni d'intrusione nei sistemi e nelle infrastrutture INAIL mediante attacchi perpetrati attraverso le reti wireless proprietarie presenti nella sede centrale dell'INAIL e nelle immediate vicinanze.

Si precisa che le attività di penetration test dovranno essere effettuate su un massimo di 85 applicazioni per ogni anno contrattuale. Le applicazioni da sottoporre a Penetration test applicativo saranno identificate dalla Funzione Sicurezza al termine del Vulnerability Assessment.

Si evidenzia che al fornitore è richiesta anche un'attività di follow-up sulle azioni correttive previste in esito ad una precedente sessione di Vulnerability Assessment e Penetration Test.

Il concorrente, nella sua Offerta Tecnica, dovrà illustrare con adeguato livello di dettaglio la metodologia e gli strumenti a supporto che intenderà utilizzare per l'esecuzione delle attività di Penetration Test. Relativamente alle attività di Vulnerability Assessment, nella formulazione della sua offerta il fornitore dovrà considerare che l'Istituto metterà a sua disposizione il prodotto McAfee Vulnerability Manager; sarà a carico del fornitore la corretta configurazione dello strumento.

DELIVERABLE ATTESI

I deliverable attesi in esito alle attività richieste sono riepilogati di seguito:

- Executive Summary, riportante i risultati più significativi dell'analisi complessiva, quali, a titolo esemplificativo e non esaustivo: il livello di rischio e di immagine, danni potenziali, facilità e reali rischi di sfruttamento delle vulnerabilità da parte di un malintenzionato, rischi legali, soluzioni gestionali e tecniche da intraprendere per ridurre il rischio, etc.. L'Executive Summary dovrà fornire anche indicazioni sulle modalità di risoluzione delle problematiche identificate, sempre utilizzando

un linguaggio business e non tecnico;

- Technical Report (uno o più documenti), dovrà contenere i dettagli tecnici particolareggiati con tutti i risultati emersi: le informazioni su tutte le vulnerabilità e problematiche di sicurezza identificate in ordine di importanza; le informazioni ed i consigli per affrontarle, nonché valutazioni sul livello reale di rischio. Questi risultati saranno oggetto di presentazione, con eventuali diapositive accompagnatorie, direttamente allo staff tecnico della DCSIT. Il documento potrà contenere termini e linguaggio specialistici, dovrà essere tuttavia di facile comprensione per lo staff tecnico, contenere una descrizione discorsiva e chiara della problematica e dell'impatto, nonché i riferimenti a documentazione ed approfondimenti (CVE o equivalenti, bollettini di sicurezza, documentazione pubblica); dove applicabile, dovranno sempre essere incluse delle dimostrazioni delle problematiche (screen shot, output di comandi, file/dati, etc.) e le procedure seguite per conseguirle (url, attacchi od exploit, etc.);

- Remediation Plan, riportante, a titolo esemplificativo e non esaustivo, l'indicazione, per ciascuna vulnerabilità individuata, della root-cause, degli interventi da porre in essere per la loro rimozione, ordinati per priorità, della stima temporale dell'intervento, della stima dell'impatto economico, organizzativo e tecnologico dell'intervento.

3.2.3.3.3. Assessment delle misure di sicurezza infrastrutturali

Scopo dell'intervento è effettuare una verifica del livello di sicurezza del network e delle soluzioni deputate alla sicurezza dello stesso.

Le attività di assessment delle misure di sicurezza infrastrutturali, volte all'analisi delle configurazioni e delle regole tecniche di sicurezza adottate per porre in sicurezza la rete, dovranno essere effettuate con frequenza annuale e dovranno essere portate a compimento entro il primo trimestre di ogni anno contrattuale.

Il fornitore deve proporre, in fase di offerta, la metodologia che intenderà adottare per verificare l'infrastruttura di rete e le configurazioni degli apparati di sicurezza con lo scopo di:

- verificare la rispondenza alle politiche definite dall'Amministrazione (ad esempio, relativamente agli apparati di sicurezza perimetrale, conformità alla politica base "Nega qualsiasi servizio eccetto quelli esplicitamente permessi", mentre nel caso dell'infrastruttura di rete, verifica del corretto posizionamento dei sistemi sulla

base dei servizi erogati);

- verificare l'efficacia delle contromisure, cercando di evidenziare possibili lacune, con riferimento allo stato dell'arte della tecnologia offerta dal mercato;
- verificare l'omogeneità nell'adozione delle contromisure, cercando di individuare possibili segmenti della rete, dei sistemi (con particolare riferimento ai dati) e degli apparati in dotazione agli utenti (pc, laptop, tablet, smartphone) non integrati nell'adozione di ogni specifica contromisura prevista dall'Amministrazione;
- testare, qualora se ne valutasse la necessità, la robustezza della misure di sicurezza, sottoponendola a tentavi di elusione;
- proporre un piano di ottimizzazione e miglioramento delle configurazioni e delle politiche e per la piena adozione di ogni contromisura.

DELIVERABLE ATTESI

I deliverable previsti sono riepilogati di seguito:

- Executive Summary, contenente la sintesi dei risultati delle attività di verifica e dell'attività di follow-up;
- Technical Report, contenente il dettaglio degli esiti delle attività di verifica, tra cui evidenza delle eventuali esigenze di rientro dalle non conformità e lo scostamento rispetto alle verifiche precedenti,
- Remediation Plan, ovvero il piano di ottimizzazione e miglioramento delle configurazioni e delle politiche e per la piena adozione di ogni contromisura.

3.2.4. Durata della fornitura – Lotto 2

Le attività previste nel Lotto 2 dovranno concludersi entro il termine massimo di 24(ventiquattro) mesi dalla "data di inizio attività", come definita nel contratto.

Il piano di lavoro della fornitura dovrà essere presentato dall'Aggiudicatario in fase di avvio della fornitura e sarà sottoposto all'approvazione della Funzione Sicurezza.

3.2.5. Deliverable della fornitura – Lotto 2

Nel paragrafo si riassumono i deliverable previsti dalla fornitura, fermo restando che INAIL si riserva di modificare formalismo e contenuti durante il corso della fornitura stessa.

Tutti i documenti dovranno essere particolarmente curati negli aspetti di:

- comprensibilità;
- accuratezza;
- adeguatezza;
- aderenza;
- modificabilità.

Tutta la documentazione dovrà essere prodotta sia su supporto cartaceo che elettronico, e consegnata anche nel formato sorgente dei singoli tools utilizzati (ad esempio Excel).

Tutti i prodotti consegnati sono soggetti ad approvazione da parte della Funzione Sicurezza; in nessun caso l'approvazione potrà avvenire per tacito assenso.

I prodotti previsti per il Lotto 2 sono elencati in

Tabella **6**, unitamente ai relativi livelli di servizio attesi ed Indici di Qualità (IQ).

Evento/Servizio	Deliverable	IQ	Livelli di Servizio
Avvio della fornitura	Piano di lavoro della fornitura	IQ05	Entro 15 (quindici) giorni lavorativi dalla stipula del contratto. Entro 5 giorni lavorativi dalla fine del semestre di riferimento per i successivi aggiornamenti
	Piano della Qualità Generale	IQ05	Entro 15 (quindici) giorni lavorativi dalla stipula del contratto
Riunione di Kick Off della fornitura	Presentazione a supporto della riunione di Kick Off della fornitura	IQ05	Entro 15 (quindici) giorni lavorativi dalla stipula del contratto
Riunione di Stato Avanzamento Lavori	Documento di Stato Avanzamento Lavori	IQ05 IQ06	Secondo le cadenze concordate con il referente dell'Amministrazione all'avvio della fornitura e riportate nel piano di lavoro del servizio
Al termine di ciascun servizio	Presentazione dei risultati per il management	IQ05	Secondo le tempistiche previste dal piano di lavoro del relativo servizio

Evento/Servizio	Deliverable	IQ	Livelli di Servizio
IT Security Audit	Piano di lavoro del servizio	IQ05	Entro 5 (cinque) giorni lavorativi dall'avvio del servizio. Entro 5 (cinque) giorni lavorativi dalla richiesta di aggiornamento da parte dell'Amministrazione o dal SAL, per i successivi aggiornamenti.
	Executive Summary	IQ05 IQ06	Secondo le tempistiche previste dal piano di lavoro del servizio
	Report di dettaglio		
	Remediation Plan		
Analisi delle attività degli Amministratori di Sistema	Piano di lavoro del servizio	IQ05	Entro 5 (cinque) giorni lavorativi dall'avvio del servizio. Entro 5 (cinque) giorni lavorativi dalla richiesta di aggiornamento da parte dell'Amministrazione o dal SAL, per i successivi aggiornamenti.
	Metodologia di audit dei log degli Amministratori di sistema	IQ05 IQ06	Secondo le tempistiche previste dal piano di lavoro del servizio
	Executive Summary		
	Technical Report		
	Remediation Plan		
ICT Security Assessment	Piano di lavoro del servizio	IQ05	Entro 5 (cinque) giorni lavorativi dall'avvio del servizio. Entro 5 (cinque) giorni lavorativi dalla richiesta di aggiornamento da parte dell'Amministrazione o dal SAL, per i successivi aggiornamenti.
VA e PT dei sistemi e delle applicazioni	Executive Summary	IQ05 IQ06	Secondo le tempistiche previste dal piano di lavoro del servizio
	Technical Report		

Evento/Servizio	Deliverable	IQ	Livelli di Servizio
web raggiungibili pubblicamente attraverso Internet	Remediation Plan		
VA e PTdei sistemi e delle applicazioni presenti sulle reti private	Executive Summary	IQ05 IQ06	Secondo le tempistiche previste dal piano di lavoro del servizio
	Technical Report		
	Remediation Plan		
Assessment delle misure di sicurezza infrastrutturali	Executive Summary	IQ05 IQ06	Secondo le tempistiche previste dal piano di lavoro del servizio
	Technical Report		
	Piano di ottimizzazione e miglioramento		
per ciascun servizio	Rapporto indicatori di qualità	IQ05	Entro 5 (cinque) giorni lavorativi dalla conclusione della verifica o della sessione

Tabella 6 - Deliverable previsti per il Lotto 2

Nel corso delle attività, potranno essere individuate altre tipologie di deliverable da consegnare i cui contenuti saranno congiuntamente concordati.

3.2.6. Gruppo di lavoro e profili professionali- Lotto 2

Il Fornitore, nell'elaborazione della sua offerta, dovrà dare una descrizione dettagliata della struttura organizzativa del progetto.

Per l'esecuzione l'esecuzione delle "attività di IT Security Audit" e delle attività di "Analisi delle attività degli Amministratori di Sistema" saranno definite "verifiche"; per l'esecuzione delle attività di "ICT Security Assessment" saranno definite "sessioni". Per le "verifiche" e per le "sessioni" si prevede un massimale in Giorni Persona (GP), quale somma delle dimensioni in giorni persona delle singole "verifiche" e "sessioni", il cui corrispettivo è calcolato sulla base dei GP della verifica o della sessione e del costo risultante dalla media ponderata delle figure professionali e della percentuale di utilizzo prevista per il relativo servizio eseguito.

I massimali di impegno previsti per l'esecuzione dei servizi richiesti sono riportati in

Tabella **7**.

Servizio	GP
IT Security Audit	280
Analisi delle attività degli Amministratori di Sistema	113
ICT Security Assessment	606

Tabella 7 - GP previsti per Servizio

Relativamente alla composizione del gruppo di lavoro, questa dovrà garantire, per ciascun servizio, almeno il mix di riferimento riportato in

Tabella **8**.

Figura professionale	Servizio		
	IT Security Audit (Impegno %)	Analisi attività AdS (Impegno %)	ICT Security Assessment (impegno %)
Security Manager	12 %	8 %	4,6 %
Security Professional Senior	0 %	0 %	7,6 %
Security Analyst Senior	55 %	46 %	74,9 %
Security Analyst Junior	33 %	46 %	12,9 %

Tabella 8 - Impegno per figura professionale e per servizio

I mix riportati nella tabella precedente sono quelli ritenuti ottimali dalla Committente, tuttavia il fornitore può 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. Eventuali scostamenti dovranno

essere preventivamente comunicati e motivati dal Fornitore in fase di pianificazione e accettati dal referente della Committente. In tal caso il corrispettivo riconosciuto al fornitore è calcolato sulla base del prezzo unitario offerto per singola figura professionale.

***

Si richiede che il gruppo di lavoro, che l'impresa proporrà per lo svolgimento dei servizi oggetto della fornitura, soddisfi i profili di seguito descritti. I curriculum vitae del personale da impiegare nei vari servizi dovranno essere resi disponibili all'Amministrazione secondo quanto previsto nelle condizioni speciali dello schema di contratto. L'Amministrazione si riserva di indicare un template per la raccolta dei curriculum vitae del personale impiegato nella fornitura. Per quanto attiene alle risorse che possiedono le certificazioni eventualmente offerte, si precisa che queste dovranno essere rese disponibili per l'intera efficacia del contratto e dovranno essere impiegate nei gruppi di lavoro che garantiscono l'erogazione dei servizi oggetto della fornitura anche senza espressa richiesta dell'Amministrazione.

Security Manager

Profilo

Laureato con anzianità lavorativa maggiore di10 anni, da computarsi successivamente alla data di conseguimento del diploma di laurea, di cui almeno 3 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 delle metodologie di vulnerability assessment, compliance management e Security Audit;
- certificazione Lead Auditor ISO 27001;
- conoscenza approfondita dei processi di Security Governance e Security Management;
- 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.

Security Professional Senior

Profilo

Laureato 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 il network (Firewall, IPS/IDS, SIEM, soluzioni anti-malware, 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;
- 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;
- comprovata esperienza in progetti analoghi.

Security Analyst Senior

Profilo

Laureato con anzianità lavorativa di almeno 7(sette) anni, da computarsi successivamente alla data di conseguimento del diploma di laurea, di cui almeno 3 (tre) anni di provata esperienza nella specifica funzione.

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

- capacità di coordinamento dei Security Analyst Junior;
- esperienza comprovata di almeno 3 (tre) anni in una o più delle seguenti aree di attività:
  - analisi delle vulnerabilità e penetration testing;
  - disegno e valutazione dei sistemi di gestione per la sicurezza.
- 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 comprovata 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;
- conoscenze approfondite di security management;
- conoscenza delle metodologie e delle tecniche per la verifica della security compliance a normative e standard interni ed esterni;
- conoscenza approfondita delle normative vigenti;
- conoscenza delle procedure di gestione della sicurezza in ambito pubblico;
- comprovata esperienza in progetti analoghi.

Security Analyst Junior

Profilo

Laureato con anzianità lavorativa di almeno 3 (tre) 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:

- conoscenza degli strumenti di Vulnerability Assessment, in particolare della Suite McAfee Vulnerability Manager, e di Penetration Test;
- partecipazione comprovata a progetti di ICT Security Assessment;
- conoscenza delle metodologie e delle tecniche per la verifica della security compliance a normative e standard interni ed esterni;
- partecipazione comprovata a progetti analoghi.

4. ESECUZIONE DELLA FORNITURA

La tipologia delle attività da svolgere e la delicatezza della materia trattata richiedono che tutte le attività dell'Aggiudicatario siano improntate a un'assoluta attenzione alla riservatezza. È inoltre fatto divieto all'Aggiudicatario di utilizzare il presente affidamento quale referenza per altri incarichi, salvo esplicita autorizzazione da parte dell'Amministrazione.

Per una descrizione delle fasi, e dei relativi deliverable di ciascun Lotto, si rimanda al paragrafo 3, fermo restando che in base alla metodologia proposta dall'Impresa

nell'Allegato 2 - Offerta Tecnica, potrà essere concordata una più ampia strutturazione delle attività.

Il corrispettivo complessivo offerto dall'Impresa si intende comprensivo di tutte le attività richieste e necessarie per l'esecuzione della fornitura. Tale corrispettivo non potrà subire aumenti neanche al variare della pianificazione effettiva rispetto a quanto inizialmente previsto o alla necessità di rielaborare i prodotti consegnati (e non ancora approvati) al fine di garantire la qualità necessaria per l'approvazione degli stessi.

L'Aggiudicatario del singolo Lotto dovrà indicare, entro 5 (cinque) giorni dalla stipula del contratto, il Responsabile della fornitura che, assumendo la piena responsabilità dei rapporti con INAIL, sarà il riferimento per gli aspetti generali e per ogni problema riguardante la fornitura stessa.

Tutte le attività di un Lotto dovranno essere svolte in collaborazione con i referenti dell'Amministrazione, secondo modalità che saranno opportunamente concordate in fase di avvio di ciascun Lotto.

La qualità della fornitura dovrà essere assicurata dall'Aggiudicatario, rispettando i criteri del proprio sistema di qualità e applicando il Piano della Qualità Generale.

L'Amministrazione si riserva di modificare le modalità di esecuzione descritte e di introdurre nuove modalità, anche in corso d'opera, dandone congruo preavviso all'Aggiudicatario. In aggiunta, tali modalità di esecuzione potranno essere congiuntamente riviste, su proposta dell'Aggiudicatario, e potranno essere concordate opportune semplificazioni o variazioni in funzione delle specificità dei singoli interventi.

L'Amministrazione si riserva di avvalersi di terzi per il supporto allo svolgimento di attività di propria competenza, ferma restando la responsabilità globale di INAIL nello svolgimento di tali attività.

4.1. Modalità di esecuzione della fornitura

La
Tabella **9** riepiloga, per ciascun Lotto, la modalità di esecuzione del singolo servizio, la relativa modalità esecutiva e la regolamentazione utilizzata.

LOTTO	Servizio	Modalità di esecuzione	Unità di misura
1	Valutazione e gestione dei rischi IT	Progettuale A corpo	Giorni per persona
	Esecuzione delle attività di IT audit	Progettuale A corpo	Giorni per persona
	Indirizzo e coordinamento	Progettuale A consumo	Giorni per persona

LOTTO	Servizio	Modalità di esecuzione	Unità di misura
	della Funzione Monitoraggio e audit IT		
2	IT Security Audit	Progettuale A corpo	Giorni per persona
	Analisi delle attività degli Amministratori di Sistema	Progettuale A corpo	Giorni per persona
	ICT Security Assessment	Progettuale A corpo	Giorni per persona

Tabella 9 - Modalità esecuzione forniture

Le attività da eseguire in modalità progettuale, in ragione della tipologia di servizio, sono scomposte in interventi e sessioni (Lotto 1) ed in verifiche e sessioni (per il Lotto 2) di responsabilità del Fornitore, cui è attribuita una dimensione e un tempo di esecuzione, suddivisi in una o più fasi, delimitate da milestone, in funzione della metodologia proposta dall'aggiudicatario in fase di offerta e di quanto concordato con l'Amministrazione.

La metrica in GP (Giorni persona) è utilizzata quale unità di misura dell'erogazione dei servizi/interventi, la cui consuntivazione avverrà comunque secondo la media ponderata delle figure professionali e della percentuale di utilizzo prevista per lo specifico servizio.

Le fasi sono delimitate da eventi (milestone), che sono gli atti, formali o sostanziali, indicati nella tabella seguente:

Attore	Milestone	Descrizione
INAIL	Richiesta stima	Richiesta al Fornitore di procedere alla stima dei tempi, dei costi e del mix di risorse necessari per il relativo intervento del singolo servizio
Fornitore	Stima	Comunicazione dei tempi, dei costi e del mix di risorse necessari per l'esecuzione dell'intervento del singolo servizio
INAIL	Autorizzazione e attivazione	Autorizzazione dell'intervento e avvio del fornitore a procedere con le attività
Fornitore	Consegna	Rilascio di eventuali prodotti di fornitura intermedi, e finali
INAIL	Approvazione	Validazione di eventuali prodotti intermedi di fornitura
INAIL	Accettazione	Validazione prodotti finali e accettazione

Attore	Milestone	Descrizione
		dell'intervento

4.2. Standard e strumenti

I deliverable in esecuzione della fornitura di ciascun Lotto dovranno rispettare gli standard documentali forniti dal referente dell'Amministrazione all'avvio della fornitura. Gli standard concordati dovranno essere formalizzati nell'apposita sezione del Piano di Qualità del progetto.

La documentazione prodotta in esecuzione della fornitura di ciascun Lotto dovrà essere compatibile con le più diffuse suite di produttività individuale (es. OpenOffice, Ms Office) e con i seguenti strumenti:

- MS Project;
- Acrobat (reader, creator, etc.);
- con eventuali altri strumenti che DCSIT riterrà opportuno utilizzare, che saranno comunicati con congruo anticipo all'Aggiudicatario.

In particolare, saranno messi a disposizione dell'Aggiudicatario, a supporto delle attività richieste per i due Lotti, gli strumenti di cui in

Tabella **10**.

Lotto	Strumento
1	Tool di mercato, strumenti proprietari in corso di implementazione o strumenti di office automation (cfr. paragrafo 3.1.3.1)
2	Geco
	McAfee Vulnerability Manager
	McAfee Policy Auditor
	McAfee Risk Advisor
	Suite ArcSight
	Compliance Pack di ArcSight

Tabella 10 - Strumenti messi a disposizione dell'Aggiudicatario

Per entrambi i Lotti si prevede di utilizzare per la pianificazione degli interventi progettuali il prodotto di mercato Clarity (CA).

L’utilizzo di ogni altro strumento dovrà essere preventivamente concordato con il referente dell’Amministrazione.

Il referente dell’Amministrazione si riserva di variare o di introdurre nuovi strumenti anche durante il corso dell'affidamento, dandone congruo preavviso all'Aggiudicatario.

Il referente dell’Amministrazione si riserva di emettere nuovi standard e/o formati dei deliverable o di modificare gli attuali anche durante il corso dell'affidamento, dandone congruo preavviso all’Aggiudicatario.

Il referente dell’Amministrazione dovrà essere messo in grado di utilizzare eventuali strumenti e metodologie di proprietà dell’Aggiudicatario.

4.3. Modalità di consegna dei deliverable

Tutti i deliverable previsti per ciascun Lotto dovranno essere consegnati in formato elettronico - anche nel formato sorgente dei singoli tool utilizzati - su CD/DVD non riscrivibili e in formato cartaceo, accompagnati dalla lettera di consegna. In alternativa la consegna potrà avvenire in formato solo elettronico, tramite posta elettronica certificata agli indirizzi che saranno indicati da INAIL.

La data di invio tramite posta elettronica e della lettera di consegna saranno le date utilizzate ai fini del calcolo degli indicatori di qualità della fornitura di cui all'Appendice.

Tutti i deliverable consegnati su CD/DVD o in via telematica dovranno essere esenti da virus.

Gli eventuali rilievi sui deliverable saranno comunicati in forma scritta, assegnando inoltre il termine per effettuare le modifiche. L’Aggiudicatario dovrà provvedere all’aggiornamento dei documenti senza oneri aggiuntivi per INAIL.

4.4. Luogo di lavoro

Per entrambi i Lotti, le attività saranno svolte prevalentemente presso le sede centrale di Roma della DCSIT. L’amministrazione si riserva la possibilità di svolgere alcune attività anche presso la sua sede secondaria, comunque collocata in Roma.
Ove il personale preposto all’esecuzione dei servizi, per entrambi i Lotti, effettuerà attività presso le sedi dell’Amministrazione, dovrà essere dotato di proprio personal computer e relativo software, comprensivo di un antivirus aggiornato. In tal caso è fatto divieto di utilizzare le stazioni di lavoro per il collegamento alla rete interna

contemporaneamente al collegamento via modem a internet o alla rete esterna. Il collegamento a Internet sarà permesso o da postazioni di lavoro individuate e messe a disposizione dell'Amministrazione oppure tramite un proxy server definito dalla DCSIT.
Eventuali costi di trasferimento e soggiorno del personale saranno a carico della Società.

Alcune attività di back-office potrebbero essere svolte presso la sede del fornitore previo accordo con l'Amministrazione.

4.5. Impiego e stabilità delle risorse

L'Aggiudicatario garantisce che tutte le risorse che impiegherà per l'erogazione dei servizi oggetto della fornitura del Lotto 1 e/o del Lotto 2, sia in fase di presa in carico dei servizi sia durante l'affidamento stesso, in caso di integrazioni e/o sostituzioni, rispondono ai requisiti minimi espressi dal presente capitolato e/o migliorativi eventualmente offerti in sede di Offerta Tecnica.

Le risorse da impiegare nelle attività previste dalle forniture, nel rispetto dei requisiti minimi definiti e/o migliorativi eventualmente offerti in sede di Offerta Tecnica, saranno individuate e presentate a INAIL in occasione della riunione di avvio della fornitura (kick-off).

In ogni caso, INAIL si riserva la possibilità di procedere ad un colloquio di approfondimento per verificare la corrispondenza alle specifiche esigenze progettuali.

Per il personale ritenuto inadeguato, qualunque sia il ruolo ed il servizio impiegato, INAIL procederà alla richiesta formale di sostituzione.

Nel Piano di lavoro del servizio (di cui al successivo paragrafo5.4), dovrà essere identificato il gruppo di lavoro assegnato stabilmente alle attività previste per ciascun servizio costituente la fornitura. E' richiesta, in particolare, la massima attenzione alla continuità delle risorse assegnate alle singole sessioni di IT Audit e di Vulnerability Assessment al fine di garantire una efficace collaborazione con il personale della DCSIT per tutta la durata dell'attività.

Si evidenzia che le eventuali sostituzioni di personale durante l'esecuzione della fornitura ovvero all'inizio della stessa dovranno essere preventivamente concordate il referente dell'Amministrazione e la sostituzione dovrà prevedere un adeguato periodo di affiancamento per la risorsa entrante.

Per il secondo anno contrattuale, l'Aggiudicatario di ciascun Lotto potrà proporre un gruppo di lavoro parzialmente diverso, fatta salva la necessità di garantire una continuità di esecuzione rispetto a quanto fatto nel primo anno contrattuale.

5. GOVERNODELLA FORNITURA

5.1. Avvio della fornitura

La Società aggiudicataria del singolo Lotto dovrà effettuare, entro 15 (quindici) giorni dalla data di stipula del contratto, la riunione di kick-off per l'illustrazione del progetto ai referenti dell'Amministrazione.

La data della riunione di kick-off costituirà la **"data di avvio della fornitura"**.

La Committente redigerà apposito verbale di avvio dell'esecuzione del contratto in contraddittorio con il Fornitore.

Contestualmente dovrà presentare la proposta di pianificazione delle attività ("Piano di lavoro della fornitura"), di cui al successivo paragrafo 6.1, per l'approvazione da parte dell'Amministrazione.

5.2. Modalità di approvazione dei deliverable

Tutte le comunicazioni inerenti l'approvazione (o mancata approvazione) dei deliverable della fornitura, sia per il Lotto 1, sia per il Lotto 2, saranno notificate formalmente al referente dell'Amministrazione. In nessun caso essa potrà avvenire per tacito assenso.

Il fornitore dovrà aggiornare i deliverable assoggettati a mancata approvazione nei tempi indicati dal referente dell'Amministrazione senza alcun onere aggiuntivo.

I tempi previsti per l'approvazione dei deliverable relativi alle attività progettuali del Lotto 1 e del Lotto 2 saranno di volta in volta concordati tra le parti e rappresentati nel Piano di Lavoro della fornitura e nel piano di lavoro del servizio.

Per tutti i deliverable della fornitura soggetti ad approvazione, la presenza di anomalie di gravità tale da impedire lo svolgimento delle attività di verifica comporta l'applicazione delle sanzioni contrattualmente previste e può comportare la risoluzione del contratto stesso.

L'approvazione dei deliverable rappresenta l'accettazione degli stessi.

5.3. Stato avanzamento lavori

Sarà cura dell'Aggiudicatario definire, all'avvio della fornitura, in accordo con il referente dell'Amministrazione, la pianificazione di incontri periodici per il monitoraggio dello stato di avanzamento dei lavori.

Durante tali incontri l'Aggiudicatario del Lotto dovrà fornire indicazioni inerenti l'avanzamento delle attività progettuali ed evidenziare eventuali problematiche riscontrate o ritardi nel completamento delle attività pianificate.

Si rimanda al paragrafo 6.3 per la descrizione delle informazioni minime che dovranno essere contenute nel documento a supporto degli incontri di Stato Avanzamento Lavori.

5.4. Piano di lavoro della fornitura

L'esecuzione ed il controllo della fornitura deve avvenire, per ciascun Lotto, con un'attività continua di gestione e monitoraggio dell'attività progettuale di cui il Piano di lavoro della fornitura è lo strumento di riferimento.

Il Piano di lavoro della fornitura è un documento che racchiude ed illustra, ad alto livello, la pianificazione dell'insieme di servizi oggetto della fornitura di un Lotto.

L'Aggiudicatario entro 15(quindici) giorni lavorativi, decorrenti dalla data di stipula del contratto, dovrà consegnare all'Amministrazione il "Piano di lavoro della fornitura" del singolo Lotto.

I successivi aggiornamenti del Piano di lavoro della fornitura del singolo Lotto dovranno avvenire con cadenza semestrale. L'Aggiudicatario dovrà consegnare all'Amministrazione Il Piano di lavoro della fornitura aggiornato entro 5 (cinque) giorni lavorativi dalla fine del bimestre di riferimento.

Il Piano di lavoro della fornitura sarà sottoposto ad approvazione da parte dell'Amministrazione che si riserva un massimo di 10 (dieci) giorni solari dalla consegna del Piano di Lavoro della fornitura per la relativa approvazione. In caso di mancata approvazione l'Amministrazione comunicherà all'Aggiudicatario i motivi del dissenso che l'Aggiudicatario si obbliga, ora per allora, a recepire aggiornando il Piano e consegnandolo all'Amministrazione stessa nel termine di 5(cinque) giorni solaride corrente dalla formalizzazione della mancata approvazione.

In ogni caso sarà cura dell'Aggiudicatario consegnare un aggiornamento del Piano di lavoro della fornitura quando si determini una variazione significativa nei suoi contenuti.

5.5. Piano di lavoro del servizio

Sulla base del Piano di lavoro della fornitura saranno prodotti alla cadenza concordata, e secondo il contenuto di massima dettagliato al paragrafo 6.2,i piani di lavoro dei servizi.

Il Piano di lavoro del servizio è un documento che racchiude l'insieme delle attività

pianificate per l'erogazione di un servizio, i tempi previsti e le risorse coinvolte, consente di estrarre delle informazioni sintetiche sullo stato di avanzamento dei lavori e di prevedere il rispetto complessivo degli obiettivi quantitativi e qualitativi. Nel Piano di lavoro si riportano il dettaglio delle attività di ogni singola fase, tempi previsti, risorse da impiegare e output da produrre.

Il Piano di lavoro del servizio dovrà essere consegnato, la prima volta, entro 5 (cinque) giorni lavorativi dall'avvio del servizio; successivamente sarà aggiornato su richiesta dell'Amministrazione, per entrambi i Lotti, quando si determina una variazione significativa nei suoi contenuti e comunque in occasione degli incontri di Stato Avanzamento Lavori. L'aggiornamento dovrà avvenire entro 5 (cinque) giorni lavorativi dalla richiesta dell'Amministrazione.

Il Piano di lavoro del servizio sarà sottoposto ad approvazione da parte dell'Amministrazione che si riserva un massimo di 10 (dieci) giorni solari dalla consegna del Piano di Lavoro del Servizio per la relativa approvazione. In caso di mancata approvazione l'Amministrazione comunicherà all'Aggiudicatario i motivi del dissenso che l'Aggiudicatario si obbliga, ora per allora, a recepire aggiornando il Piano e consegnandolo all'Amministrazione stessa nel termine di 5(cinque) giorni solari decorrente dalla formalizzazione della mancata approvazione.

5.6. Piano della Qualità generale

Il Piano della Qualità generale del singolo Lotto, redatto dall'Aggiudicatario sulla base del proprio manuale di qualità e dello schema esposto al paragrafo 6.3, costituirà il riferimento per le attività di verifica e validazione svolte dall'Aggiudicatario all'interno dei propri gruppi di lavoro.

Entro 15 (quindici) giorni lavorativi dalla data di stipula del contratto, l'Impresa si obbliga a consegnare il Piano della Qualità generale.

Il Piano della Qualità generale sarà sottoposto ad approvazione da parte dell'Amministrazione che si riserva un massimo di 10 (dieci) giorni solari dalla consegna del Piano della Qualità generale per la relativa approvazione. In caso di mancata approvazione, l'Amministrazione comunicherà all'Impresa i motivi del dissenso, quest'ultima si obbliga entro 10 (dieci) giorni solari dalla comunicazione a recepire i rilievi e a consegnarlo all'Amministrazione.

Il Piano della Qualità Generale del singolo Lotto dovrà essere aggiornato a seguito di significativi cambiamenti di contesto in corso d'opera, o comunque su richiesta del referente dell'Amministrazione, ogni qualvolta lo reputi opportuno.

Nell'esecuzione delle attività contrattualmente previste per il singolo Lotto, l'Aggiudicatario dovrà, inoltre:

- Rispettare i principi di assicurazione e gestione della qualità della norma EN ISO 9001;
- Attenersi ed essere conforme a quanto previsto dal Piano della Qualità Generale, da eventuali Piani della qualità dei singoli interventi approvati e dal proprio Sistema di gestione della qualità.

Indicatori di qualità della fornitura

L'insieme degli indicatori di qualità della fornitura, da inserire nel Piano della Qualità Generale, comprende come nucleo base quelli elencati nell'Appendice. Laddove è presente un valore numerico, questo è da intendersi come requisito minimo atteso da INAIL (valore di soglia).

L'Aggiudicatario è tenuto a rendicontare i risultati della misurazione di tutti gli indicatori di qualità per tutta la durata contrattuale attraverso il Rapporto indicatori di qualità.

Tale rapporto dovrà essere redatto dall'Aggiudicatario e dovrà essere consegnato nei tempi previsti in

Tabella **2**, per il Lotto 1, e in

Tabella **6**, per il Lotto 2.

Il Rapporto indicatori di qualità costituirà complessivamente il riferimento per la valutazione del rispetto dei requisiti di qualità, al fine dell'applicazione delle penali (paragrafo 6.5).

Durante l'intero periodo contrattuale ciascun indicatore di qualità potrà essere riesaminato su richiesta dell'Amministrazione e/o dell'Aggiudicatario; il riesame potrà derivare da nuovi strumenti di misurazione non disponibili alla data di stipula del contratto e/o dall'adeguamento delle metodiche atte alla rilevazione dei singoli indicatori di qualità che sono risultate non efficaci.

5.7. Vincoli temporali sulle consegne

Di seguito vengono indicati i vincoli temporali sui termini di consegna:

- del Piano di lavoro della fornitura;
- del Piano di lavoro del servizio(e connesso Stato avanzamento lavori);
- del Rapporto indicatori qualità;

- del Piano della Qualità generale.

Il Piano di lavoro della fornitura per il singolo Lotto dovrà essere consegnato entro 15 (quindici) giorni lavorativi dalla data di stipula del contratto.

Successivamente il Piano di lavoro della fornitura sarà aggiornato con frequenza semestrale, entro 5 (cinque) giorni lavorativi dalla fine del semestre di riferimento.

Il Piano di lavoro del servizio per il singolo Lotto dovrà essere consegnato entro 5 (cinque) giorni lavorativi dall'avvio del servizio. Successivamente dovrà essere aggiornato entro 5 (cinque) giorni lavorativi dalla richiesta dell'Amministrazione e in occasione dei SAL.

In linea generale, tutti i deliverable previsti quali risultati delle attività pianificate di un servizio dovranno essere consegnati nei tempi previsti dal Piano di lavoro del servizio e formalmente sottoposti all'approvazione del referente dell'Amministrazione.

In caso vengano formalizzate osservazioni a fronte delle quali occorra apportare variazioni di contenuto del Piano di lavoro della fornitura del Lotto e/o del Piano di Lavoro del servizio, questo dovrà essere riconsegnato entro 5(cinque) giorni solari dalla formalizzazione delle osservazioni stesse, salvo diverso termine assegnato dal referente dell'Amministrazione in tale sede.

In caso vengano formalizzate osservazioni a fronte delle quali occorra apportare variazioni di contenuto allo Stato avanzamento lavori del Lotto, questo dovrà essere riconsegnato entro 5 (cinque) giorni solari dalla formalizzazione delle osservazioni stesse salvo diverso termine assegnato dal referente dell'Amministrazione in tale sede.

Il Piano della Qualità generale del Lotto dovrà essere consegnato entro 15 (quindici) giorni lavorativi dalla data di stipula del contratto.

In caso vengano formalizzate osservazioni a fronte delle quali occorra apportare variazioni di contenuto al Piano della qualità generale, questo dovrà essere riconsegnato entro 10 (dieci) giorni solari dalla formalizzazione delle osservazioni stesse salvo diverso termine assegnato dal referente dell'Amministrazione in tale sede.

L'Aggiudicatario del Lotto dovrà inoltre, entro 5 (cinque) giorni lavorativi dall'accettazione di ogni intervento del singolo servizio, consegnare al referente dell'Amministrazione il Rapporto indicatori di qualità.

5.8. Indicatori di qualità

Per ciascun Lotto di fornitura sono fissati gli specifici indicatori di qualità riportati nell'Appendice.

5.9. 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) da INAIL 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

6. CONTENUTI DEI DELIVERABLE

Tutto il materiale prodotto in esecuzione della fornitura prevista sia per il Lotto 1 che per il Lotto 2, sarà di esclusiva proprietà dell'INAIL, che ne potrà disporre liberamente.

Tutti i deliverable realizzati nell'ambito dell'affidamento dovranno rispondere ai requisiti stabiliti nel Piano della Qualità Generale.

6.1. Piano di lavoro della fornitura

Sarà redatto ed aggiornato un Piano di lavoro dell'intera fornitura, contenente la pianificazione ad alto livello di tutti i servizi del Lotto.

Il piano di lavoro della fornitura dovrà riportare per ciascun servizio, a titolo indicativo e non esaustivo, le seguenti informazioni:

- nome, descrizione e, se significativo, relativo stato (sospeso, cancellato, ecc.);
- Direzioni / Aree INAIL coinvolte;
- nominativo del referente dell'Aggiudicatario per il servizio;
- descrizione del servizio;
- milestone dei singoli servizi, indicanti le date di consegna, previste ed effettive, dei deliverable;
- impegno, stimato ed effettivo, secondo la metrica applicabile (FTE o giorni persona) dell'effort progettuale, suddiviso per servizio e per figura professionale;
- risorse da impiegare nei singoli servizi;
- gantt.

Il formato di redazione del Piano di lavoro della fornitura verrà concordato con DCSIT.

6.2. Piano di lavoro del servizio

Sarà redatto ed aggiornato un Piano di lavoro del servizio, contenente, per ogni servizio del Lotto, il dettaglio di attività, tempi e stime di impegno.

Coerentemente con le caratteristiche delle singole attività, per ciascun servizio si dovranno riportare, a titolo indicativo e non esaustivo, le seguenti informazioni:

- nome, descrizione e, se significativo, relativo stato (sospeso, cancellato, ecc.);
- Direzioni / Aree INAIL coinvolte;
- nominativo del referente dell'Aggiudicatario per l'attività;
- descrizione dell'intervento;
- elenco delle fasi e delle singole attività con relative date di inizio e fine, previste ed effettive;
- prodotti delle singole fasi, con relative date di consegna, previste ed effettive;
- impegno, stimato ed effettivo, secondo la metrica applicabile (FTE o giorni persona) dell'effort progettuale, ove applicabile suddiviso per fase/attività e per figura professionale;
- risorse da impiegare nelle singole attività;
- gantt delle attività.

Si precisa che le date finali delle varie fasi, devono essere comprensive anche dell'eventuale tempo di approvazione dei prodotti.

Il formato di redazione del Piano di lavoro del Servizi verrà concordato con DCSIT.

6.3. Documento di Stato Avanzamento Lavori

Lo stato di avanzamento lavori di ogni singolo servizio di ogni singolo Lotto dovrà riportare, a titolo indicativo e non esaustivo, le seguenti informazioni:

- percentuale di avanzamento delle singole attività;
- nome, descrizione dell'intervento;
- stato delle attività alla data in termini di (attività significative concluse nel periodo in esame, attività significative in corso e/o previste a breve);
- razionali di ripianificazione, scostamento eventuale delle date, dell'impegno e del volume;
- vincoli/criticità e relative azioni da intraprendere e/o intraprese.

6.4. Piano di qualità della fornitura

Il Piano della Qualità Generale è il documento che precisa le modalità operative, le risorse

e le sequenze delle attività relative alla qualità della fornitura.

Il Fornitore del Lotto dovrà predisporre un Piano della Qualità Generale che:

- fornisca lo strumento per collegare i requisiti minimi contrattualmente richiesti, con le procedure generali del sistema qualità del fornitore già esistenti;
- espliciti le disposizioni organizzative e metodologiche adottate dal fornitore, allo scopo di raggiungere gli obiettivi tecnici e di qualità contrattualmente definiti;
- dettagli i metodi di lavoro messi in atto dal fornitore, facendo riferimento o a procedure relative al proprio sistema, e per ciò descritte nel manuale qualità (ove presente); o a procedure sviluppate per lo specifico contrattuale, a supporto delle attività in esso descritte, in questo caso da allegare al piano;
- garantisca il corretto e razionale evolversi delle attività contrattualmente previste, nonché la trasparenza e la tracciabilità di tutte le azioni messe in atto dalle parti in causa, il fornitore, il committente, l'eventuale organismo di ispezione accreditato dall'INAIL.

Nella redazione del Piano di qualità della fornitura, l'Aggiudicatario del Lotto avrà come guida lo schema di seguito descritto.

1) Scopo e campo di applicazione

Riportante:

- lo scopo ed il campo di applicazione del Piano della Qualità Generale;
- una sintesi dei suoi contenuti.

2) Documenti di riferimento e applicabili

Riportante:

- l'elenco delle appendici che sono parte integrante del piano
  (ad es. standard di documenti del fornitore, standard di rendicontazione degli indicatori di qualità, procedure/istruzioni definite o personalizzate per il contratto, ecc.);
- l'elenco dei documenti applicabili per quanto esposto nel presente Piano della Qualità Generale ma non allegati al piano (ad es. Manuale della qualità, procedure, processi, *istruzioni, ecc.*).

3) Organizzazione e Responsabilità

Riportante:

- l'organigramma del gruppo di lavoro impegnato con l'identificazione del/dei:
  - responsabile della fornitura;
  - responsabile della Qualità della fornitura;

- responsabile della definizione ed attuazione del Piano della Qualità Generale;
- responsabile delle attività di controllo da eseguire;
- responsabile della gestione della documentazione.

- la "matrice delle responsabilità" che, per ciascun ruolo definito nell'organigramma della fornitura, assegna una precisa responsabilità.

4) Metodi, tecniche e strumenti

Riportante:

- le metodologie, le tecniche e gli strumenti da utilizzare per l'erogazione dei servizi della fornitura;
- gli standard da utilizzare per redigere i documenti della fornitura.

5) Requisiti di qualità

Riportante:

- gli obiettivi di qualità e gli indicatori di qualità (riportati nell'Appendice), e gli eventuali indicatori di qualità aggiuntivi, proposti in sede di offerta, ed accettati dall'Amministrazione;
- gli obiettivi di prestazione della fornitura, articolati in un subset degli indicatori di qualità e negli indicatori di risultato aziendale;
- la Procedura di valutazione della qualità (definisce o referenzia la procedura per la valutazione della qualità dei prodotti e/o servizi).

6) Registrazioni della qualità

Riportante:

- l'elenco di tutte le registrazioni della qualità, sia quelle previste dal sistema di gestione qualità adottato, sia specificatamente previste per l'attuazione del contratto, necessarie a supportare le attività di gestione del contratto e di assicurazione della qualità;
- le modalità per soddisfare i requisiti di leggibilità, di archiviazione, di rintracciabilità, di disponibilità e di riservatezza delle registrazioni;
- le modalità di conservazione delle registrazione e il periodo di mantenimento.

7) Riesami, verifiche e validazioni

Riportante:

- l'elenco dei controlli da effettuare per le attività della fornitura;
- le modalità di esecuzione dei controlli.

8) Segnalazione di problemi ed azioni correttive

descrive le specifiche procedure previste per la gestione di problemi quali malfunzionamenti e non conformità

9) Controllo dei sub-fornitori

delinea le procedure e gli accorgimenti da adottare il controllo dei sub-fornitori

10) Raccolta e salvaguardia dei documenti

descrive la procedura per la gestione, conservazione e salvaguardia della documentazione della fornitura, nonché il periodo di mantenimento previsto della documentazione

11) Formazione ed addestramento

descrive le attività di formazione inerenti al contratto. Tali attività riguardano gli eventuali aggiornamenti tecnici a cui sottoporre le risorse dell'Aggiudicatario che lavorano per l'espletamento del contratto

12) Glossario

contiene le abbreviazioni, gli acronimi, le definizioni, che saranno utilizzati all'interno del documento

6.5. Rapporto indicatori di qualità

Il Rapporto indicatori di qualità dovrà essere redatto dall'Aggiudicatario del Lotto e dovrà contenere la rendicontazione delle misurazioni effettuate sugli indicatori di qualità riportati nel Piano della Qualità Generale approvato dall'Amministrazione.

Il Rapporto indicatori di qualità costituirà il riferimento per la valutazione del rispetto dei requisiti di qualità al fine della corresponsione dei corrispettivi e dell'applicazione delle penali.

Il Rapporto indicatori di qualità del singolo servizio previsto dal Lotto dovrà essere predisposto in forma incrementale e consegnato entro 5 (cinque) giorni lavorativi dall'inizio del mese successivo al trimestre di rilevazione (secondo le tempistiche di cui alla

Tabella **2**, per il Lotto 1, e di cui alla

Tabella **6**, per il Lotto 2, salvo puntuali richieste da parte dell'Amministrazione), pena l'applicazione delle penali di cui all'art. 14 S.

6.6. Executive Summary

In esito allo svolgimento dei servizi previsti, l'Aggiudicatario dovrà produrre un Executive Summary per la descrizione sintetica dei risultati delle attività.

L'Executive Summary dovrà riassumere, in ordine di importanza, i risultati più significativi dell'attività svolta da un punto di vista manageriale e sarà oggetto di presentazione, con diapositive accompagnatorie, direttamente alla Direzione.

Il documento dovrà essere conciso, di facile lettura per management e personale non tecnico e concentrarsi sugli aspetti strategici e dovrà fornire anche indicazioni sulle modalità di risoluzione delle problematiche identificate, sempre utilizzando un linguaggio business e non tecnico.

La struttura ed i contenuti del documento saranno definiti dall'aggiudicatario di concerto con il referente dell'Amministrazione.

6.7. Technical report

In esito allo svolgimento dei servizi previsti, l'Aggiudicatario dovrà produrre un Technical Report, costituito da uno o più documenti/allegati, per la descrizione dettagliata delle attività effettuate, della metodologia impiegata e dei risultati ottenuti destinata al personale tecnico delle strutture organizzative di DCSIT.

Il Technical Report dovrà contenere i dettagli tecnici particolareggiati con tutti i risultati emersi e le informazioni ed i consigli per affrontare le eventuali problematiche emerse in esito alle attività progettuali.

I risultati saranno oggetto di presentazione, con diapositive accompagnatorie, direttamente allo staff tecnico della DCSIT.

Il documento potrà contenere termini e linguaggio specialistici, dovrà essere tuttavia di facile comprensione per lo staff tecnico, contenere una descrizione discorsiva e chiara della problematica nonché i riferimenti a documentazione ed approfondimenti per la risoluzione della stessa.

La struttura ed i contenuti del documento saranno definiti dall'Aggiudicatario del Lotto di concerto con il referente dell'Amministrazione.

6.8. Remediation Plan

Il remediation plan è il documento riportante l'indicazione, ad alto livello, delle possibili contromisure tecnologiche, organizzative e/o procedurali da porre in essere per eliminare

le problematiche, le cause di non conformità e/o le vulnerabilità rilevate.

Il Remediation Plan deve contenere, come minimo, le seguenti informazioni:

- la descrizione della problematica rilevata;
- l'indicazione della root-cause;
- la descrizione dell'attività da porre in essere per risolvere la problematica;
- una stima temporale dell'intervento;
- una stima qualitativa (Alto, medio, basso, sulla base di criteri concordati con il referente dell'Amministrazione) dell'impatto economico, organizzativo e tecnologico dell'intervento;
- la priorità di implementazione dell'intervento.

6.9. Presentazioni

Le presentazioni sono finalizzate a fornire al middle e al top management delle Strutture Organizzative di DCSIT le informazioni utili alla comprensione delle attività svolte nell'esecuzione del servizio, delle logiche e delle sistematicità previste dalla metodologia al fine di meglio interpretare e comprendere i risultati ottenuti e gli interventi di miglioramento indicati.

Per ogni Lotto e per ogni fase/servizio è richiesta la presentazione dei risultati con diversi contenuti a seconda della platea a cui dovrà essere indirizzata.

La Società dovrà provvedere alla progettazione di ogni singola presentazione, provvedendo altresì alla preparazione del materiale da distribuire ai partecipanti.

Le presentazioni dovranno essere utilizzate per illustrare, a titolo esemplificatio e non esaustivo, i seguenti argomenti/deliverable:

- Executive summary (diapositive elettroniche e documento);
- Punti focali sull'applicazione della metodologia (diapositive elettroniche e documento);
- Stato avanzamento lavori (diapositive elettroniche, tabelle, verbali incontri);
- Risultati dell'attività e criticità riscontrate (diapositive elettroniche e documento).

7. DIMENSIONI MASSIME DEI SINGOLI SERVIZI

I servizi offerti per ciascun Lotto dovranno essere dimensionati tenuto conto del perimetro della fornitura, descritto nei paragrafi 3.1.2 e 3.2.2, rispettivamente per il Lotto 1 e per il Lotto 2, e dei profili professionali richiesti per l'esecuzione degli stessi, descritti al paragrafo 3.1.6 e al paragrafo 3.2.6, rispettivamente per il Lotto 1 e per il Lotto 2.

8. RISORSE IMPIEGATE

Tutte le figure professionali che svolgeranno le attività oggetto del presente Capitolato Tecnico dovranno rispondere alle caratteristiche descritte nel paragrafo3.1.6 e 3.2.6, rispettivamente per il Lotto 1 e per il Lotto 2, ovvero a quelle migliorative eventualmente offerte e presteranno la loro attività conformemente al mix espresso.

L'Impresa si obbliga a consegnare i curricula delle figure professionali che svolgeranno le attività oggetto della fornitura, così come descritte ai paragrafi 3.1.3 e 3.2.3 per il Lotto 1 e per il Lotto 2 rispettivamente, nonché di quelle impegnate nell'erogazione dei servizi in giorni persona presso le sedi dell'Amministrazione, unitamente alle certificazioni previste, ovvero dichiarate in sede di Offerta, nonché alla documentazione idonea a provare il rapporto di lavoro in essere con l'Impresa stessa in ragione di quanto dichiarato in sede di offerta tecnica, entro le scadenze contrattuali. Tale obbligo dovrà essere rispettato anche in corso di fornitura, qualora si debba provvedere all'inserimento di una nuova risorsa, entro i termini contrattuali, salvo diverso termine indicato dall'Amministrazione.

L'Amministrazione si riserva la facoltà di effettuare dei colloqui alle risorse di cui al capoverso precedente. Il Fornitore dovrà mettere a disposizione gratuitamente le suddette risorse per un colloquio di almeno un'ora presso la sede dell'INAIL, entro i termini contrattuali.

Ove l'Amministrazione ritenga la figura professionale proposta non idonea allo svolgimento dell'attività contrattuale, la medesima ne darà comunicazione all'Impresa, la quale si impegna a procedere ad una nuova proposta entro 10 (dieci) giorni solari. La valutazione di tale nuovo curriculum segue la disciplina illustrata.

L'impresa prende atto ed accetta che le risorse impegnate nell'erogazione dei servizi dovranno essere in possesso delle certificazioni richieste nel Capitolato tecnico (per tale intendendosi anche le Appendici) e di quelle indicate in sede di offerta per l'intera durata contrattuale. Pertanto al variare dei percorsi di certificazione, l'impresa stessa dovrà garantire l'effettuazione degli eventuali aggiornamenti necessari al mantenimento delle certificazioni stesse, garantendo la continuità di servizio per le risorse impegnate nell'erogazione dei servizi.

Fermo restando l'obbligo di assicurare la prosecuzione e la continuità delle prestazioni contrattuali, anche garantendo un adeguato periodo di controllo e di affiancamento non inferiore a 30 (trenta) giorni lavorativi, l'Aggiudicatario del Lotto, nel caso in cui debba provvedere alla sostituzione di una risorsa coinvolta nella esecuzione delle prestazioni contrattuali, dovrà comunicare la motivazione all'Amministrazione e consegnare a quest'ultima, con un preavviso di 30 (trenta) giorni solari, il curriculum della nuova figura

professionale.

L'Amministrazione ha la facoltà di richiedere la sostituzione di unità di personale addetto alle prestazioni contrattuali del singolo Lotto qualora fossero ritenute dalla medesima non idonee alla perfetta esecuzione del presente contratto. In tal caso, l'Aggiudicatario del Lotto dovrà proporre una nuova figura professionale. L'esercizio da parte dell'Amministrazione di tale facoltà non comporterà alcun onere per la stessa.

Nell'ipotesi di cui ai precedenti due capoversi, l'Amministrazione si riserva la facoltà di valutare l'idoneità della nuova figura professionale proposta entro il termine di 10 (dieci) giorni lavorativi dal ricevimento del relativo curriculum.

Ove l'Amministrazione ritenga la figura professionale proposta non idonea allo svolgimento dell'attività contrattuale, la medesima ne darà comunicazione all'Aggiudicatario del Lotto, la quale si impegna a procedere ad una nuova proposta entro il termine di 5 (cinque) giorni lavorativi dalla predetta comunicazione.

Si precisa che le nuove figure professionali devono avere attestati ed esperienze, in tipologia e durata, non inferiori alla risorsa da sostituire.

In caso di valutazione positiva, comunicata per iscritto, da parte dell'Amministrazione del curriculum presentato o di decorrenza del termine di 10 (dieci) giorni lavorativi, l'Aggiudicatario si obbliga a provvedere alla sostituzione della figura professionale entro 7 (sette) giorni solari dalla comunicazione di assenso o dalla decorrenza del predetto termine o nel diverso termine indicato dall'Amministrazione.

Nel caso in cui l'Aggiudicatario proceda alla sostituzione della figura professionale senza la necessaria preventiva valutazione e autorizzazione dell'Amministrazione, quest'ultima si riserva, previa contestazione dell'addebito e valutazione delle deduzioni addotte dall'Impresa e da questa comunicate all'Amministrazione nel termine massimo di 5 (cinque) giorni solari, di applicare una penale così come indicato nel Contratto. L'Aggiudicatario prende atto che l'Amministrazione, al fine di ottenere la massima qualità professionale del servizio reso, si riserva la facoltà di verificare, in ogni momento dell'esecuzione del contratto, la corrispondenza della qualità del servizio e delle figure professionali effettivamente impiegate rispetto a quanto indicato nei paragrafi 3.1.6 e 3.2.6, rispettivamente per il Lotto 1 ed il Lotto 2.

In caso di inadempimento da parte dell'Impresa degli obblighi di cui al presente capitolo, l'Amministrazione applicherà le sanzioni previste nel contratto sulla base degli indicatori di qualità **IQ01**, **IQ02**, **IQ03, IQ04** e **IQ07** di cui all'Appendice, fermo restando il diritto al risarcimento del danno, ed avrà facoltà di dichiarare risolto di diritto il presente contratto.

9. VERIFICA DI CONFORMITÀ

In corso di contratto l'Amministrazione effettuerà la verifica di conformità delle prestazioni, volta a certificare che le prestazioni contrattuali siano eseguite a regola d'arte sotto il profilo tecnico-funzionale.

Tali verifiche verranno avviate per il Lotto 1:

a) relativamente alla "Valutazione e gestione dei rischi IT", di cui all'art. 1 S comma 1 lett. a), anche con riferimento alla verifica degli Indicatori di qualità applicabili riportati nell'Appendice al Capitolato Tecnico, entro 20 (venti) giorni solari dall'ultimazione dell'attività stessa;
b) per quanto attiene all'"Esecuzione delle attività di IT Audit", di cui all'art. 1 S comma 1 lett. b), anche relativamente alla verifica degli Indicatori di qualità riportati nell'Appendice al Capitolato Tecnico, entro 20 (venti) giorni solari dalla conclusione del trimestre di riferimento;
c) per quanto attiene al servizio di "Supporto Specialistico per l'attività di Indirizzo e coordinamento della funzione di AUDIT" di cui all'art. 1 S comma 1 lett. b), anche relativamente alla verifica degli Indicatori di qualità riportati nell'Appendice al Capitolato Tecnico, entro 20 (venti) giorni solari dal trimestre di riferimento.

Tali verifiche verranno avviate per il Lotto 2:

a) con riferimento al servizio di "IT Security Audit" e relativamente alla verifica degli Indicatori di qualità come riportati nell'Appendice al Capitolato tecnico, entro 20 (venti) giorni dall'ultimazione della "verifica";

b) con riferimento al servizio di "Analisi delle attività degli Amministratori di Sistema" e relativamente alla verifica degli Indicatori di qualità come riportati nell'Appendice al Capitolato tecnico, entro 20 (venti) giorni dall'ultimazione della "verifica";

c) con riferimento del servizio di "ICT Security Assessment" e relativamente alla verifica degli Indicatori di qualità come riportati nell'Appendice al Capitolato tecnico, entro 20 (venti) giorni dall'ultimazione della "sessione".

Le verifiche saranno ripetute in corso di esecuzione del contratto, per le prestazioni continuative.

La Verifica di conformità verrà effettuata con le modalità ed entro i termini indicati nel Contratto e si intende positivamente superata solo in caso le prestazioni contrattuali siano state eseguite a regola d'arte sotto il profilo tecnico e funzionale, in conformità e nel rispetto delle condizioni, modalità, termini e prescrizioni espresse nel presente Capitolato tecnico.

Nel caso in cui, durante la verifica, venissero rilevate anomalie in ragione dei livelli di servizio richiesti, sarà emessa una penale in funzione degli indicatori applicabili ai casi riscontrati.

Nel caso in cui, durante la verifica, venissero rilevate anomalie che secondo l'Amministrazione, per numero e/o gravità, non permettano il prosieguo delle attività, la verifica verrà interrotta e riprenderà ex novo dal momento in cui l'Amministrazione riterrà ripristinate le sopracitate anomalie. In caso di interruzione della verifica, per quanto attiene gli Indicatori di qualità, sarà emessa una penale in funzione degli indicatori applicabili ai casi riscontrati.

L'Aggiudicatario dovrà provvedere, senza oneri aggiuntivi per l'Amministrazione, all'eliminazione degli eventuali vizi e difformità riscontrati durante le operazioni di verifica, secondo i tempi che saranno concordati con l'Amministrazione.

Si precisa che tutti gli oneri derivanti dalla verifica di conformità si intendono a carico dell'Aggiudicatario.

Delle operazioni di Verifica di conformità verrà redatto apposito processo verbale. Nel caso di esito positivo della verifica di conformità la data del relativo verbale verrà considerata quale "Data di accettazione del servizio", per la relativa prestazione contrattuale, da parte dell'Amministrazione.

L'Amministrazione rilascerà il certificato di verifica di conformità, e l'Amministrazione potrà procedere allo svincolo della cauzione prestata dall'Aggiudicatario, qualora risulti che l'Aggiudicatario ha regolarmente eseguito le prestazioni contrattuali nel rispetto di quanto previsto:

- dall'art.322, 323 del D.P.R. 5 ottobre 2010, n.207;
- dagli art. 315 e seguenti del D.P.R. 5 ottobre 2010, n.207.

Su richiesta dell'Aggiudicatario, l'Amministrazione emetterà il certificato di esecuzione prestazioni dei servizi (CES), coerentemente al modello predisposto dall'Autorità per la Vigilanza sui contratti pubblici. Il certificato verrà emesso solo a seguito della verifica di conformità delle prestazioni rese, nel rispetto delle prescrizioni contrattuali e della normativa vigente.