Oggetto: Gara per l'acquisizione di supporto tecnico-metodologico alle attività di AUDIT della Direzione Centrale per i Servizi Informativi e Telecomunicazione e alle attività di controllo dell'efficacia delle misure di sicurezza IT dell'INAIL – ID 1466

Errata Corrige e Chiarimenti

L'Errata Corrige e i chiarimenti della gara sono visibili sul sito www.consip.it

Errata Corrige

N. 1 - Allegato 4 – Condizioni speciali dello Schema di contratto per il Lotto 1
L'art. 16S comma 11 delle condizioni speciali dello schema di contratto Lotto 1 "Si precisa che le fatture di cui al comma 1 lett. dovranno essere prodotte unitamente a relativo verbale positivo di verifica di conformità di cui al precedente art. 12 S, comma 9" deve intendersi sostituito come segue:
"Si precisa che le fatture di cui ai precedenti commi 1, 2, e 3, dovranno essere prodotte unitamente al relativo verbale positivo di verifica di conformità di cui al precedente art. 12 S, comma 9".

N. 2 - Disciplinare di gara
Ai criteri J 9 per il Lotto 1 e J 9 per il Lotto 2 si aggiunge la seguente precisazione:
"Per il raggiungimento della percentuale di cui alle precedenti lettere a) e b), alle risorse assunte presso il Concorrente, o società facenti parte dell'RTI o Consorzio, con contratto di lavoro subordinato saranno equiparati i soci dell'Impresa concorrente, o delle società facenti parte dell'RTI o Consorzio, che svolgano attività lavorativa nell'Impresa, o nelle società facenti parte dell'RTI o Consorzio, per l'esecuzione dell'appalto".
L'Allegato 2 Lotto 1 punto 3.9 e l'Allegato 2 Lotto 2 punto 3.9 si intendono integrati come segue "Al raggiungimento della percentuale oggetto di impegno concorrono anche le risorse che rivestono il ruolo di soci dell'Impresa concorrente, o delle società facenti parte dell'RTI o Consorzio, che svolgano attività lavorativa nell'Impresa, o nelle società facenti parte dell'RTI o Consorzio, per l'esecuzione dell'appalto".

N. 3 – Allegato 5 - Capitolato Tecnico
I paragrafi 3.1.6 Lotto 1 e 3.2.6 Lotto 2 sono integrati come segue: "Per ogni figura professionale il possesso del diploma di laurea potrà essere sostituito dal possesso di *"cultura equivalente"*, che corrisponde a 5 (cinque) anni di esperienza lavorativa addizionali rispetto a quelli richiesti dal capitolato Tecnico per la corrispondente figura professionale, di cui due (sempre addizionali rispetto a quelli eventualmente richiesti) nella specifica funzione".

***

Chiarimenti

1) **Domanda**
   Si richiede se per le certificazioni relative ai Senior Security Analyst previsti per il Lotto II al requisito ID j6 è possibile considerare valide anche certificazioni equivalenti come la CEH (Certified Ethical Hacker) o la GPEN (GIAC Penetration Tester) che garantiscono gli stessi requisiti e la stessa preparazione richiesta per la OPST di OSSTMM"
   Risposta
   Ai fini dell'assegnazione del punteggio di cui al criterio j6 lettere c) e d) per il Lotto 2, non è possibile considerare valide le certificazioni CEH (Certified Ethical Hacker) e GPEN (GIAC Penetration Tester).
   Si conferma pertanto quanto scritto sul Disciplinare di gara relativamente al criterio di merito tecnico j6, lettere c) e d) del Lotto II, e cioè che per ottenere il punteggio di merito ivi espresso, le risorse che soddisfano il profilo di Security Analyst Senior, devono essere in possesso della certificazione OSSTMM-OPST.

2) **Domanda**
   Documento cui si riferisce il quesito: Bando di gara d'appalto - Paragrafo documento: III.2.2 - capacità economica e finanziaria - Capoverso documento: 1 capoverso, lett. a) - Pagina documento: 4 - Frase oggetto del quesito: "aver realizzato, complessivamente negli ultimi tre esercizi finanziari approvati alla data di pubblicazione del presente Bando..." - Chiarimento richiesto: Considerando che il bando è stato pubblicato in

data 17/03/2014 e che i bilanci aziendali relativi all'anno 2013 vengono approvati entro 120 giorni dalla chiusura dell'esercizio (e quindi entro il 30/04/2014), si richiede se il triennio da tenere in considerazione (per le aziende che approvano il bilancio 2013 il 30/04/2013) sia quello 2011 - 2012 – 2013.

Risposta

Il bando di gara risulta pubblicato sulla GURI il 21 marzo 2014.

Nel caso di impresa il cui bilancio 2013 sia stato approvato dopo il 21 marzo 2014 il triennio da tenere in considerazione è quello 2010-2011-2012.

Nel caso di impresa il cui bilancio 2013 sia stato approvato prima del 21 marzo 2014 il triennio da tenere in considerazione è quello 2011-2012-2013.

3) **Domanda**

Documento cui si riferisce il quesito: Bando di gara d'appalto - Paragrafo documento: III.2.2 - capacità economica e finanziaria - Capoverso documento: 1 capoverso, lett. a) - Pagina documento: 4 - Frase oggetto del quesito: "aver realizzato, complessivamente negli ultimi tre esercizi finanziari approvati alla data di pubblicazione del presente Bando, un fatturato specifico per la prestazione di servizi di Valutazione e gestione dei rischi IT e attività di IT Audit non inferiore a Euro 480.000,00 = (quattrocentoottantamila/00), IVA esclusa" - Chiarimento richiesto: Considerando che spesso le attività richieste sono comprese in contratti più generali, del tipo "Servizi per la Sicurezza IT" ovvero "servizi per l'implementazione di sistemi di gestione della sicurezza delle informazioni (SGSI)", "attività di supporto per IT Governance" si chiede di confermare se tali contratti possano essere considerati per il raggiungimento del requisito di capacità economica e finanziaria.

Risposta

Premesso che i "Servizi di Valutazione e gestione dei rischi IT e attività di IT Audit" individuano autonome prestazioni, il requisito di cui al punto III.2.2 lett. a) è soddisfatto nel caso in cui il Fornitore abbia eseguito negli ultimi tre esercizi finanziari approvati alla data di pubblicazione del Bando, un fatturato specifico per la prestazione di servizi di "Valutazione e gestione dei rischi IT e attività di IT Audit" non inferiore a Euro 480.000,00, IVA esclusa. In sede di comprova ex art. 48, comma 1 e 2, D. Lgs. n. 163/2006, il concorrente dovrà produrre la documentazione di cui al paragrafo 6 del Disciplinare di gara idonea a provare l'esecuzione nel periodo di riferimento delle suddette prestazioni e non di altre più generiche.

4) **Domanda**

Documento cui si riferisce il quesito: Bando di gara d'appalto - Paragrafo documento: III.2.3 – capacità tecnica - Capoverso documento: 1 capoverso, lett. a) - Pagina documento: 5 - Frase oggetto del quesito: "avere eseguito regolarmente, nei tre anni antecedenti la data di pubblicazione del Bando di Gara, 1 (un) contratto stipulato con committenti pubblici o privati avente ad oggetto servizi di "Esecuzione delle attività di IT Audit", per un valore complessivo non inferiore a Euro 120.000,00 (centoventimila/00), IVA esclusa.." - Chiarimento richiesto: Si chiede conferma che i tre anni antecedenti la data di pubblicazione del bando sia il triennio 2011 - 2012 – 2013

Risposta

Per il requisito di cui al punto III.2.3 lett. a) del bando di gara il triennio di riferimento va dal 21 marzo 2011 al 21 marzo 2014; in tale periodo temporale il concorrente deve aver regolarmente eseguito **un unico contratto** avente ad oggetto servizi di "Esecuzione delle attività di IT Audit" per un valore complessivo non inferiore a 120.000,00 Euro, IVA esclusa.

Si precisa inoltre che non è necessario che l'esecuzione del contratto si sia protratta per tutto il triennio sopra individuato. E' pertanto soddisfatto il requisito anche nel caso in cui, a titolo esemplificativo, la regolare esecuzione del singolo contratto per un valore complessivo non inferiore a 120.000,000 Euro, IVA esclusa, sia avvenuta nel biennio 2012-2013, nel solo 2012 o nel periodo compreso tra il 2013 e il 20 marzo 2014.

5) **Domanda**

Documento cui si riferisce il quesito: Allegato 2 - lotto 1 - Offerta tecnica - Paragrafo documento: 3.5 Miglioramento dei requisiti minimi previsti per il profilo di manager - Capoverso documento: 1 capoverso, lett. a) - Pagina documento: 5 - Frase oggetto del quesito: "Il Concorrente descriva la proposta di miglioramento del requisito minimo, relativo al profilo di Manager, in particolare esprima l'impegno a garantire per tale profilo

a) Il possesso della certificazione PMP PMI"

Chiarimento richiesto: Si chiede se sia equivalente il possesso di certificazioni di Project Management quali Prince2, ISIPM o IPMA

Risposta

Ai fini dell'attribuzione del punteggio di cui al criterio J 5 lett. a) (per il Lotto 1) il concorrente dovrà esprimere l'impegno a garantire per il profilo di manager il possesso della certificazione PMP PMI, come previsto nel Disciplinare di gara.
Non sono ammesse altre certificazioni ai fini dell'ottenimento di un punteggio migliorativo previsto per tale criterio per il Lotto 1.

6) Domanda

Documento cui si riferisce il quesito: Allegato 2 - lotto 1 - Offerta tecnica - Paragrafo documento: 3.9 Team Operativi - Capoverso documento: 1 capoverso, lett. a) - Pagina documento: 6 - Frase oggetto del quesito: a) almeno il 30 % di risorse componenti i gruppi di lavoro impiegati nell'erogazione dei servizi per il Lotto 1 sia assunto presso il Concorrente, o società facenti parte dell'RTI o del Consorzio, con contratto di lavoro subordinato; - Chiarimento richiesto: Si chiede di specificare quali siano le fattispecie di contratto di lavoro subordinato e se in queste fattispecie rientrino:
1) i soci di società che siano anche amministratori;
2) contratti di tipo CO.CO.PRO "

Risposta

Premesso che il criterio in esame non contiene requisiti di accesso alla gara, ma elementi migliorativi utili ai fini dell'attribuzione di punteggio tecnico, si precisa che per contratto di lavoro subordinato si intende il contratto tramite il quale il lavoratore, assunto presso l'imprenditore, si obbliga mediante retribuzione a collaborare nell'impresa, prestando il proprio lavoro intellettuale o manuale alle dipendenze e sotto la direzione dell'imprenditore. In tali fattispecie non rientrano i contratti di tipo CO.CO.PRO.
Si veda per i soci dell'Impresa concorrente quanto precisato con l'Errata corrige n. 2.

7) Domanda

Allegato 5 - Capitolato tecnico al paragrafo 3.1.6 Gruppo di lavoro e profili professionali - Lotto 1 si richiedono alcuni requisiti ad esempio:

a. profilo di manager: anzianità lavorativa minima di 10 anni di cui almeno 3 nella specifica funzione, certificazione CISA
- profilo di consulente senior: anzianità lavorativa minima di 7 anni di cui almeno 3 nella specifica funzione, certificazione CISA

Allegato 2 Offerta tecnica - Lotto 1 al paragrafo 3.5 si richiede il miglioramento dei requisiti minimi previsti:

- profilo cli manager: certificazione PMP PMI, possesso certificazione CISM o CRISC
- Profilo di consulente senior: certificazione ITIL Foundation v.3, ITIL Expert v.3

In relazione a quanto indicate esponiamo le seguenti domante:

- profilo di Manager- Lotto 1.
  In relazione alla figura di Manager quali sono i requisiti obbligatori?
  Quelli descritti nel capitolato tecnico - allegato 5? les anzianità, certificazione CISA).
  Gli altri requisiti richiesti nell' allegato 2 di offerta tecnica " miglioramento dei requisiti minimi" (certificazione PMI, certificazione CISM/CRISC) sono obbligatori per accedere alla gara?
  Eventualmente se vengono proposti diversi profili di Manager può un profilo di manager garantire una certificazione (es. CISA) ed un altro profilo di Manager garantire la certificazione CRISC/CISM?
- Profilo consulente senior - Lotto 1. In relazione alla figura di consulente senior i requisiti di certificazione ITIL Foundation v.3 ed ITIL Expert v.3 sono facoltativi o obbligatori?
  Anche in questo caso sono aggiuntivi rispetto alla certificazione CISA richiesta dal capitolato tecnico?
  La certificazione CISA è obbligatoria?
  Eventualmente se vengono proposti diversi profili di senior consultant può un profilo di senior consultant garantire una certificazione (es. CISA) ed un altro profilo di senior consultant (o eventualmente anche di Manager) garantire la certificazione ITIL Foundation/Expert?

Risposta

I requisiti descritti nel Capitolato Tecnico (per entrambi i Lotti) sono obbligatori ed indispensabili per eseguire le prestazioni oggetto di gara.
I requisiti indicati nel Disciplinare (per entrambi i Lotti), tra i criteri di valutazione delle offerte tecniche e nell'Allegato 2 Lotto 1 e nell'Allegato 2 Lotto 2 al Disciplinare stesso, non sono necessari per la partecipazione alla gara ma, se offerti del concorrente, consentiranno l'attribuzione del punteggio previsto per il corrispondente criterio. In particolare,

- **profilo di Manager - Lotto 1**; in relazione alla figura di **Manager** sono requisiti obbligatori per l'esecuzione del Contratto tutti quelli descritti nel capitolato tecnico - allegato 5.

I requisiti richiesti nell'Allegato 2 Lotto 1, di offerta tecnica "miglioramento dei requisiti minimi" e nel Disciplinare di gara al criterio j5, non sono obbligatori per accedere alla gara.
Per ottenere tale punteggio premiante, previsto nel suddetto criterio, è necessario che un Manager abbia (cap. 6 del Disciplinare di gara), in aggiunta ai requisiti del Capitolato Tecnico, anche:

a) possesso della certificazione PMP PMI (1,5 punti);
b) possesso della certificazione CISM o CRISC unitamente alla certificazione PMP PMI (3 punti).

Si precisa che l'eventuale assegnazione del punteggio di cui al punto b) non comporta l'assegnazione del punteggio di cui al punto a).

E' possibile che il concorrente proponga un gruppo di lavoro che preveda due manager di cui il primo, certificato PMP PMI, assumerà il ruolo di PM (con conseguente attribuzione del punteggio aggiuntivo di cui sopra), mentre il secondo, certificato CISA, effettuerà/coordinerà operativamente tutte le attività previste dal Lotto 1 riconducibili a tale certificazione.

- **profilo di Consulente senior - Lotto 1**; in relazione alla figura di **Consulente senior** i requisiti di certificazione ITIL Foundation v.3 ed ITIL Expert v.3 sono facoltativi e, se offerti, garantiscono l'attribuzione del seguente punteggio migliorativo (cap. 6 del Disciplinare di gara):
  a) impegno a garantire che almeno una delle risorse che soddisfano il profilo di Consulente Senior, sul totale delle risorse che compongono il gruppo di lavoro proposto dal concorrente, sia in possesso della certificazione ITIL Foundation v.3 (0,75 punti);
  b) impegno a garantire che almeno due delle risorse che soddisfano il profilo di Consulente Senior, sul totale delle risorse che compongono il gruppo di lavoro proposto dal concorrente, sia in possesso della certificazione ITIL Foundation v.3 (1,5 punti);

  Si precisa che i punteggi di cui al punto a) e di cui al punto b) sono tra loro alternativi.

  c) impegno a garantire che almeno una delle risorse che soddisfano il profilo di Consulente Senior, sul totale delle risorse che compongono il gruppo di lavoro proposto dal concorrente, sia in possesso della certificazione ITIL Expert v.3 (0,75 punti) ;
  d) impegno a garantire che almeno due delle risorse che soddisfano il profilo di Consulente Senior, sul totale delle risorse che compongono il gruppo di lavoro proposto dal concorrente, sia in possesso della certificazione ITIL Expert v.3 (1,5 punti).

  Si precisa che i punteggi di cui al punto c) e di cui al punto d) sono tra loro alternativi.
  E' possibile che il concorrente proponga un gruppo di lavoro che preveda più consulenti senior di cui uno o due, certificato/i ITIL Foundation v.3 (con conseguente attribuzione del punteggio previsto), mentre gli altri certificati CISA.
  Resta fermo che tutti i profili di Consulente senior proposti devono essere in possesso della certificazione CISA, come indicato nel par. 3.1.6 del Capitolato tecnico, se eseguiranno le attività oggetto della certificazione.

8) Domanda

III.2.2) Capacità economica e finanziaria
b) Lotto 2: aver realizzato, complessivamente negli ultimi tre esercizi finanziari approvati alla data di pubblicazione del presente Bando, un fatturato specifico per la prestazione di servizi di IT Security Audit e ICT Security Assessment non inferiore a Euro 500.000,00. I fatturati presentati a copertura del requisito possono riguardare servizi professionali per l'adeguamento alla normativa del Garante?

Risposta

Premesso che il quesito non risulta del tutto chiaro, si precisa che per il raggiungimento del fatturato specifico di cui al punto III.2.2 lett. b) del bando di gara, possono rilevare servizi professionali relativi alla disciplina del Decreto Legislativo n.° 196/2003 - Codice in materia di protezione dei dati personali, e successive modificazioni, integrazioni e Provvedimenti applicabili al contesto di INAIL, solo nel caso in cui risultino riconducibili ai servizi di IT Security Audit descritti nel Capitolato Tecnico.

9) Domanda

III.2.3) Capacità tecnica
b) Lotto 2: avere eseguito regolarmente, nei tre anni antecedenti la data di pubblicazione del Bando di Gara, 1 (un) contratto stipulato con committenti pubblici o privati avente ad oggetto servizi di "ICT Security Assessment", per un valore complessivo non inferiore a Euro 100.000,00 (centomila/00), I VA esclusa.
Il numero di contratti da presentare è 3 o 1?

Risposta

Sulla base di quanto stabilito al punto III.2.3) lett. b) Capacità tecnica del Bando di gara per il Lotto 2 il concorrente deve aver eseguito regolarmente, nei tre anni antecedenti la data di pubblicazione del Bando di

Gara, **1 (un) unico contratto** stipulato con committenti pubblici o privati avente ad oggetto servizi di "ICT Security Assessment", per un valore complessivo non inferiore a Euro 100.000,00, IVA esclusa.
Il contratto deve essere 1 (uno) solo, deve essere stato regolarmente eseguito tra il 21 marzo 2014 (data di pubblicazione del bando di gara) ed il 21 marzo 2011 e per un valore complessivo non inferiore a Euro 100.000,00 (centomila/00), IVA esclusa.
Non è necessario che l'esecuzione si sia protratta in ogni anno del triennio di riferimento; è soddisfatto il requisito nel caso cui il concorrente abbia eseguito regolarmente 1 (un) contratto con le suddette caratteristiche in un periodo compreso, a titolo esemplificativo, tra il 2012 ed il 2013 o dal 1 gennaio 2013 al 20 marzo 2014.
Non è soddisfatto il requisito nel caso in cui il concorrente abbia eseguito 3 (tre) contratti nel triennio di riferimento che abbiano tutti e tre complessivamente valore non inferiore a Euro 100.000,00 (centomila/00) IVA esclusa. Si rileva che nel caso in cui il concorrente sia sprovvisto del requisito potrà far ricorso all'istituto dell'"avvalimento" secondo quanto stabilito nel Disciplinare di gara al capitolo 4 e nella normativa di riferimento.

10) Domanda
Documento di gara: Gara AUDIT INAIL - Allegato 5 - Capitolato tecnico
Lotto 2: - Profili professionali : Manager Manager, Security Professional Senior, Security Analyst Senior, Security Analyst Junior.
Per tutte le figure indicate è richiesto il possesso del diploma di laurea, sono accettate figure professionali non laureate ma con "cultura equivalente" e se si come deve essere considerata la relativa corrispondenza?
Risposta
Si veda l'Errata corrige N. 3.

11) Domanda
A pagina 5 dei Disciplinare di gara, viene richiesta la registrazione ai sistema dell'AVCPass e la creazione del PassOE. Abbiamo avviato la procedura di creazione del cruscotto del PassOE. Abbiamo cercato la procedura di affidamento cui si intende partecipare tramite CIG. Il sistema al momento risponde: 'Il CIG indicato non è gestito dal sistema AVCpass'. Utilizzando la ricerca avanzata, la gara viene intercettata, ma non si riesce a selezionare. La procedura che prevede il pagamento della tassa AVCP relativa alla gara in oggetto è regolarmente attiva. Abbiamo verificato con il support dell' AVCpass, ci ha consigliato di segnalarvi il problema constatato.
Risposta
In ragione della facoltà prevista nel Disciplinare ove si prevede che Consip "si riserva di procedere alla verifica circa il possesso dei requisiti inerenti la presente iniziativa tramite la BDNCP" si precisa che per la procedura in oggetto la Consip non provvederà al completamento delle informazioni relative alla "Scheda dei Requisiti di Partecipazione" in quanto effettuerà la verifica del possesso dei requisiti degli operatori economici secondo le previgenti modalità.
La produzione del PASSOE all'interno della Busta A "Documenti" per la presente iniziativa è, pertanto, facoltativa. La mancata registrazione presso il servizio AVCpass, nonché l'eventuale mancata trasmissione del PASSOE, non comportano l'esclusione dalla presente procedura.

12) Domanda
Relativamente ai requisito di capacità economica e finanziaria, chiediamo conferma che i concorrenti riuniti in raggruppamento temporaneo debbano possedere tali requisiti ed eseguire le prestazioni nella % corrispondente alla quota di partecipazione al raggruppamento, fermo restando che la mandataria debba possedere tali requisiti in misura maggioritaria.
Risposta
Non si conferma. Fermo restando che la mandataria debba possedere i requisiti di capacità economica e finanziaria in misura maggioritaria in senso relativo e debba eseguire le prestazioni in misura maggioritaria in senso relativo, non è necessario vi sia corrispondenza tra possesso del suddetto requisito da una parte e quote di partecipazione al raggruppamento e quote di esecuzione dall'altra.

13) Domanda
In merito a quanto riportato al Paragrafo 2 punto a) a pag.7 del Disciplinare di gara, al fine di dimostrare l'insussistenza delle cause di esclusione ex art. 38, comma 1, lettere b), c) e m) ter dei D.lgs. n. 163/2006 per tutti i soggetti indicati a pagina 8, si chiede conferma che:
- il Legale rappresentante possa dichiarare per sé e per gli altri soggetti individuati all'art. 38 comma 1 lett. b) c) e m-ter) l'insussistenza delle cause di esclusione previste al medesimo articolo?

- nel caso fosse possibile che il Legale rappresentante dichiari per sé e per conto di tutti gli altri soggetti, é corretto utilizzare come modello l'Allegato 1 Bis adattandolo a questa richiesta?

Risposta

Si conferma che il Legale rappresentante possa dichiarare per sé e per gli altri soggetti individuati all'art. 38 comma 1 lett. b) c) e m-ter) e puntualmente elencati a pag. 8 e 9 del Disciplinare di gara l'insussistenza delle cause di esclusione previste al medesimo articolo. A tal fine è sufficiente che il concorrente utilizzi il solo Allegato 1 in virtù del quale, il sottoscrittore titolare dei poteri necessari per impegnare il concorrente deve rendere le dichiarazioni di cui al punto 2 (lettere a, b, c, d, e, f), al punto 3, e al punto 7 (lettere b, c, d, e), ferma restando la necessaria compilazione di tutti gli altri campi previsti nel medesimo Allegato. Come previsto nel Disciplinare di gara la produzione dell'Allegato 1 bis da parte dei su richiamati soggetti è prevista a pena di esclusione qualora il soggetto che sottoscrive la Dichiarazione conforme all'*Allegato 1* al presente Disciplinare renda la stessa esclusivamente nei propri confronti.

14) Domanda

All.2 OT_General : Con riferimento alla Relazione Tecnica da compilare a cura del Fornitore, viene indicato che la stessa deve essere contenuta entro le 70 pagine (formato DIN A4). Non è chiaro al Fornitore se esistono e debbono essere tenuti in considerazione ulteriori requisiti "formali" in merito alle caratteristiche della offerta tecnica medesima (es. dimensioni carattere, interlinea, etc.). RIFERIMENTO DOCUMENTO: "ALLEGATO 2 - LOTTO 1, FAC SIMILE OFFERTA TECNICA, pag.3; ALLEGATO 2 - LOTTO 2 FAC SIMILE OFFERTA TECNICA, pag.3"

Risposta

Non sono prescritti ulteriori requisiti formali per la redazione della Relazione tecnica oltre quelli indicati nel Disciplinare di gara e negli allegati 2, per i due Lotti. Ferma restando la necessaria leggibilità dell'offerta, è preferibile che la dimensione del carattere utilizzato sia almeno 9 e l'interlinea almeno singola; si ribadisce che l'estensione della relazione deve essere contenuta nelle 70 pagine.

15) Domanda

ALL.5 CSO_General: Con riferimento ai Gruppi di Lavoro ed ai profili professionali richiesti per i Lotti 1 e 2, ci potrebbe essere il caso in cui il Fornitore disponga di risorse il cui profilo risponde ai requisiti previsti per una o più figure sia del Lotto 1 che del Lotto 2. Nel caso in cui ciò risulti compatibile con i carichi di lavoro stimati ed i tempi previsti di esecuzione delle attività, può il Fornitore proporre una stessa risorsa per figure diverse per i due Lotti? (es. Manager per Lotto 1 e Security Manager per Lotto 2). RIFERIMENTO DOCUMENTO: ALLEGATO 5 - 3.1.6 Pag.25 e 3.2.6 pag.48

Risposta

Si conferma. Restano fermi i vincoli, gli obblighi e le tempistiche esecutive previste nella documentazione di gara per entrambi i Lotti anche in ordine ai requisiti professionali delle risorse da utilizzare negli appalti.

16) Domanda

ALL.5 CSO_General: Nella sezione 4.1 in cui si declinano le modalità di esecuzione della fornitura per i due Lotti, viene specificato che "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". Non è chiaro al Fornitore quali siano le ricadute operative di tale inciso. RIFERIMENTO DOCUMENTO: ALLEGATO 5 - 4.1 pag.54

Risposta

La determinazione del corrispettivo avviene in ragione del numero dei giorni persona definiti, delle tariffe professionali, del mix indicato per il servizio dalla documentazione di gara.

17) Domanda

ALL.5 CSO_Lotto1: Con riferimento all'esecuzione delle attività di IT Audit (All.5 - 3.1.3.2), si fa riferimento al numero massimo di processi da sottoporre ad attività di IT audit (20 processi il primo anno, 33 il secondo anno). Non è chiaro al Fornitore se l'elenco dei processi da auditare sarà fornito direttamente da INAIL oppure l'Aggiudicatario dorvà formulare una proposta da sottoporre al vaglio e valutazione di INAIL. In questo secondo caso, si chiarisca quali elementi saranno messi a disposizione del Fornitore per formulare la proposta. RIFERIMETNO DOCUMENTO: ALLEGATO 5 - 3.1.3.2 pag.19

Risposta

INAIL in fase di avvio contrattuale fornirà l'elenco dei processi da sottoporre ad Audit e per ognuno di essi la descrizione di dettaglio corredata del flow chart e della matrice di responsabilità.

18) Domanda

ALL.5 CSO_Lotto1: Nella sezione 3.1.3.1 in cui si declina l'oggetto della fornitura per il Lotto 1, viene specificato che "I deliverable attesi in esito alle attività previste sono riepilogati di seguito: (...omissis...) 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". Non è chiaro al Fornitore se sarà richiesto all'Aggiudicatario solo la pianificazione degli interventi di remediation ovvero un'attività completa di project management in ambito remediation, comprensivo quindi anche del monitoraggio dell'execution dell'action plan. RIFERIMENTO DOCUMENTO: ALLEGATO 5 - LOTTO 1 3.1.3.1 pag.17

Risposta

Si richiede al Fornitore la sola attività di pianificazione degli interventi di remediation e di follow-up sui risultati di precedenti attività di audit.

19) Domanda

ALL.5 CSO_Lotto1: Nella sezione 3.1.6 in cui si declina il Gruppo di Lavoro ed i profili professionali per il Lotto 1, viene specificato che per l'esecuzione delle attività di "Valutazione e gestione dei rischi IT" si prevede un unico intervento progettuale, ma, pur essendo fornito l'impegno % delle risorse, non viene indicato il numero di giorni persona previste per la loro esecuzione. Non è chiaro al Fornitore se la mancata indicazione delle GP è dovuta al fatto che l'attività è da intendersi "a corpo" - come precisato nelle modalità di esecuzione della fornitura - e come tale CONSIP non ritiene necessario stimare il massimale di impegno previsto. RIFERIMENTO DOCUMENTO: ALLEGATO 5 - LOTTO 1 3.1.6 pag. 25

Risposta

L'attività di "Valutazione e gestione dei rischi IT" è da intendersi "a corpo"; fermi i requisiti professionali indicati nel Capitolato Tecnico, non è previsto un massimale specifico in termini di giorni lavorativi; resta fermo il termine ultimo per l'esecuzione dell'attività richiesta.

20) Domanda

ALL.5 CSO_Lotto2: Nella sezione 3.1.3.1 in cui si declina l'oggetto della fornitura per il Lotto 2, viene specificato che "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". Non è chiaro al Fornitore se sarà richiesto all'Aggiudicatario solo la pianificazione degli interventi di remediation ovvero un'attività completa di project management in ambito remediation, comprensivo quindi anche del monitoraggio dell'execution dell'action plan. RIFERIMENTO DOCUMENTO: ALLEGATO 5 - LOTTO 2 3.2.3.3.1 pag.41

Risposta

Si veda la risposta alla domanda n. 18.

21) Domanda

ALL.5 CSO_Lotto2: Nella sezione 3.2.3.1 in cui si declina l'oggetto della fornitura per il Lotto 2, viene specificato che "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". Non è chiaro al Fornitore se si sta richiedendo di garantire dei follow up su remediation plan relativi ad audit precedenti all'esecuzione dei servizi di cui alla presente procedura (cfr. precedente campagna di controllo). RIFERIMENTO DOCUMENTO: ALLEGATO 5 - LOTTO 2 3.2.3.1 pag.34

Risposta

Si richiede al Fornitore di effettuare dei follow-up sia su remediation plan precedenti all'esecuzione dei servizi di cui alla presente procedura, sia sui remediation plan in esito ai servizi di cui alla presente procedura.

22) Domanda

ALL.5 CSO_Lotto2: Nella sezione 3.2.3.3.2 in cui si declina l'oggetto della fornitura per il Lotto 2, viene specificato che "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". Avendo il PT interno in ambito n.ro 85 applicazioni per anno, non è chiaro al Fornitore come verranno selezionate le stazioni client, se su proposta dell'Aggiudicatario ovvero su indicazione di INAIL. RIFERIMENTO DOCUMENTO: ALLEGATO 5 - LOTTO 2 3.2.3.3.2 pag.41

Risposta

Le stazioni client saranno selezionate da INAIL e comunicate all'Aggiudicatario.

23) Domanda

ALL.5 CSO_Lotto2: Nella sezione 3.2.3 in cui si declina l'oggetto della fornitura per il Lotto 2, viene specificato che le attività di VA-PT sono semestrali, mentre l'assessment dell'infrastruttura è annuale. Non è chiaro al Fornitore, ed in tal sede si chiede conferma, se CONSIP sta richiedendo di effettuare un totale di: n.ro 4 VAPT Interni e n.ro 4 VAPT Esterni; n.ro 2 security assessment infrastrutturali. RIFERIMENTO DOCUMENTO: ALLEGATO 5 - LOTTO 2, 3.2.3 pagg. 33

Risposta

Tale interpretazione è corretta: l'Istituto richiede l'esecuzione di 2 (due) VAPT e 1 (uno) security assessment infrastrutturale per ciascun anno di validità contrattuale.

24) Domanda

ALL.5 CSO_Lotto2: Nella sezione 3.2.3.1 in cui si declina l'oggetto della fornitura per il Lotto 2, viene specificato che "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: (... omissis...) Decreto Legislativo n° 82/2005 - Codice dell'Amministrazione Digitale, e successive modificazioni ed integrazioni". Stante il più recente aggiornamento del C.A.D. avvenuto con D. lgsl. 235/2010, non è chiaro al Fornitore se si stia richiedendo la compliance a quest'ultimo decreto ovvero, per motivi non precisati, si intenda far riferimento solo al D.Lgs. 82/05. RIFERIMENTO DOCUMENTO: ALLEGATO 5 - LOTTO 2, 3.2.3.1 pag.34.

Risposta

Il decreto legislativo 30 dicembre 2010 n. 235, pubblicato nel Supplemento ordinario n. 8 alla Gazzetta Ufficiale n. 6 del 10 gennaio 2010, rientra tra le "successive modificazioni ed integrazioni" di cui al capoverso indicato nella domanda del Fornitore avendo, di fatto, modificato sostanzialmente il testo del CAD introdotto nel 2005 con il decreto legislativo 7 marzo 2005, n. 82, ed è pertanto da tenere in debita considerazione ai fini delle attività di verifica della conformità al CAD.

25) Domanda

ALL.5 CSO_Lotto2: Nella sezione 3.2.3.3 in cui si declina l'oggetto della fornitura per il Lotto 2, viene specificato che "i test saranno eseguiti su sistemi e reti in esercizio". Non è chiaro al Fornitore se, ai fini di una verifica esaustiva e reale, sarà possibile durante il Vulnerability Assessment effettuare test sulle stesse applicazioni in ambiente di test (ad es. per estrarre informazioni utili all'attacco). RIFERIMENTO DOCUMENTO: ALLEGATO 5 - LOTTO 2, 3.2.3.3 pag.37

Risposta

Le attività di VAPT dovranno essere effettuate in ambiente di produzione.

26) Domanda

ALL.5 CSO_Lotto2: Nella sezione 3.2.3.3 in cui si declina l'oggetto della fornitura per il Lotto 2, viene specificato che "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)". Non è chiaro al Fornitore se si sta chiedendo specificatamente di effettuare test DOS e, in caso positivo, come CONSIP intende gestire da un punto di vista contrattuale gli eventuali impatti (es. possibilità che un disservizio si prolunghi oltre il tempo stimato). RIFERIMENTO DOCUMENTO: ALLEGATO 5 - LOTTO 2, 3.2.3.3 pag. 37

Risposta

L'Istituto non richiede specificatamente al Fornitore di effettuare delle attività di test volte a verificare la "resilienza" della propria infrastruttura ad attacchi DOS o DDOS. Il Fornitore, qualora rilevi l'esigenza di effettuare dei test che potrebbero comportare blocchi o disservizi alla normale operatività di INAIL, dovrà, come riportato nel capitolato tecnico, concordarle con l'Istituto a cui illustrerà l'effettiva necessità di effettuare tali tipologie di test, le modalità operative, i rischi associati e l'eventuale supporto tecnico/organizzativo che dovrà essere predisposto congiuntamente al fine di ridurre i rischi associati al test.

27) Domanda

ALL.5 CSO_Lotto2: Nella sezione 3.2.3.3.1 in cui si declina l'oggetto della fornitura per il Lotto 2, viene specificato che tra le attività minime è inclusa la "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". Non è chiaro al Fornitore se, ai fini di una simulazione il più possibile esaustiva e

realistica, sarà possibile effettuare anche attività con un profilo di rischio (es. installazione software sulle macchine di produzione). RIFERIMENTO DOCUMENTO: ALLEGATO 5 - LOTTO 2, 3.2.3.3.1 pag.39
Risposta
Non è consentita l'installazione di software, connettori, plug-in, etc. sulle macchine di produzione

28) Domanda
DISCIPLINARE_Criteri di valutazione OT: Il criterio di valutazione j3 (formazione e aggiornamento) recita che "L'impresa, ai fini dell'attribuzione del punteggio, deve inoltre produrre un template del/i deliverable attraverso cui verrà fornita, nel corso della fornitura, evidenza della applicazione della modalità proposta". Non risulta chiaro al Fornitore quale sia il deliverable rispetto al quale CONSIP si aspetta la produzione di uno o più template esemplificativi. RIFERIMENTO DOCUMENTO: Disciplinare di Gara, pag. 45
Risposta
Il Fornitore dovrà produrre un template di deliverable (es: corso e-learning, presentazioni, …) che, unitamente e coerentemente alla descrizione della soluzione organizzativa e operativa fornita, consentirà all'Istituto di valutare la capacità del Fornitore di garantire la formazione continua delle risorse che ha impegnato nella fornitura.

29) Domanda
DISCIPLINARE_Criteri di valutazione OT: Il criterio di valutazione j4 (monitoraggio delle attività contrattuali) recita che "Soluzione proposta che il Fornitore si impegna ad adottare per eseguire periodiche rilevazioni sull'andamento delle attività affidate con la produzione di report periodici.
Saranno valutati in particolare: il grado di copertura di servizi/attività contrattuali; gli strumenti di reportistica, la rappresentazione grafica". Non risulta chiaro al Fornitore quale sia l'aspettativa di CONSIP rispetto al punto "grado di copertura dei servizi/ attività contrattuali". RIFERIMENTO DOCUMENTO: Disciplinare di Gara, pag. 45
Risposta
Il Fornitore dovrà riportare il livello di granularità delle attività di rilevazione dell'andamento delle attività affidategli.

30) Domanda
DISCIPLINARE_Requisiti di bando: Nella premessa del Disciplinare di Gara si evidenzia la necessità di procedere al caricamento della documentazione probatoria dei requisiti di carattere generale nonché tecnico-organizzativo ed economico finanziario esclusivamente attraverso la BDNCP, strumento attraverso cui CONSIP può verificare tali requisiti. Si evince di seguito che la mancata registrazione presso il servizio AVCpass, nonchè l'eventuale mancata trasmissione del PASSOE, non comportano di per se e salvo quanto oltre previsto l'esclusione dalla procedura di gara.
Stante quanto sopra riportato, non è chiaro al Fornitore se la suddetta documentazione probatoria debba essere caricata obbligatoriamente prima della scadenza della procedura di gara oppure se si debbano attendere precise indicazioni da CONSIP (procedura Art.48 Comma1 Codice degli Appalti eo Aggiudicazioni). Inoltre, non è chiaro a cosa si riferisca l'inciso "e salvo quanto oltre previsto". DOCUMENTO DI RIFERIMENTO: Disciplinare di Gara, pagg. 5-6.
Risposta
Si veda la risposta alla domanda n. 11.

31) Domanda
Capitolato d'oneri. Registrazione al Sistema AVCPASS e utilizzazione della Banca Dati Nazionale Contratti Pubblici – pag. 6. Ambito dl riferimento AVCPASS - Attribuzione PASSOE.
Si chiede di confermare che, la mancata registrazione presso il servizio AVCpass e il successivo inserimento nella Busta amministrativa dei PASSOE in fase di offerta ed altresì nelle fasi successive di gara, non sia ritenuto necessario e pertanto non comporti l'esclusione dalla presente procedura di gara.
Risposta
Si conferma. Si veda anche la risposta alla domanda n. 11.

32) Domanda
Capitolato tecnico. Capitolo 3.2.3.3.2 VA e PT su sistemi e applicazioni presenti sulle reti private. Servizio di Vulnerability Assessment e Penetration Test.
Si chiede di confermare che per eseguire le attività di VA e PT, sia possibile utilizzare strumenti del fornitore.
Risposta
Come riportato nel Capitolato Tecnico, pag. 43, per l'esecuzione delle attività di Penetration Test il Fornitore dovrà illustrare con adeguato livello di dettaglio gli strumenti e la metodologia che intenderà utilizzare

mentre per le attività di Vulnerability Assessment il Fornitore dovrà utilizzare il prodotto McAfee Vulnerability Manager che sarà messo a disposizione dall'Istituto.

33) Domanda

Allegato 4 - Condizioni Speciali Lotto 2. Art. 16 S Fatturazione. Ambito dl riferimento Pagamenti.
Si chiede dl confermare che trovino applicazione le nuove disposizioni ex D.Lgs. 192/2012 che prevedono un termine di pagamento pari a 30gg data ricevimento fattura ovvero di indicare eventuale diverso termine e relativa motivazione.

Risposta

Si conferma quanto previsto nell'allegato 4, condizioni speciali dello schema di contratto art. 16 S, comma 13, per il Lotto 1, ove si precisa che "*i termini di pagamento delle predette fatture, corredate della documentazione di cui al precedente comma 11, saranno definiti secondo le modalità di cui alla vigente normativa, D.Lgs 231/2002 e smi.*" e art. 16 S, comma 9, per il Lotto 2, ove si precisa che "*i termini di pagamento delle predette fatture, corredate della documentazione di cui al precedente comma 7, saranno definiti secondo le modalità di cui alla vigente normativa, D.Lgs 231/2002 e smi*". Il D. Lgs. 9 ottobre 2002, n. 231, modificato dal D. Lgs. n. 192/2012 prevede all'art. 4 comma 2 che il termine di pagamento è: "[…], *trenta giorni dalla data di ricevimento da parte del debitore della fattura o di una richiesta di pagamento di contenuto equivalente*". Nel medesimo comma è inoltre fatto "s*alvo il disposto dei commi […] 4 e 5*"; il comma 4 prescrive che "*Nelle transazioni commerciali in cui il debitore è una pubblica amministrazione le parti possono pattuire, purché in modo espresso, un termine per il pagamento superiore a quello previsto dal comma 2, quando ciò sia giustificato dalla natura o dall'oggetto del contratto o dalle circostanze esistenti al momento della sua conclusione. In ogni caso i termini di cui al comma 2 non possono essere superiori a sessanta giorni. La clausola relativa al termine deve essere provata per iscritto*".

34) Domanda

Allegato 4 - Condizioni Speciali Lotto 2 Paragrafo Art. 14 S Penali.
Si chiede di confermare che l'ammontare massimo di penali applicabili al presente appalto/contratto non potrà in nessun caso superare il 10% del valore complessivo dei presente appalto/contratto, in linea con quanto previsto dal DPR 207/2010 art. 145.

Risposta

L'ammontare delle penali inflitte potrà superare il 10% del corrispettivo totale, fatta salva l'applicabilità dei criteri elaborati in materia dalla giurisprudenza.

35) Domanda

Non rilevandosi menzione alcuna relativamente ai Codice Etico Consip pubblicato sul relativo sito web, si chiede di confermare che il concorrente sia tenuto all'osservanza dei principi in esso Contenuti.

Risposta

Non si conferma.

36) Domanda

LOTTO 1: Nell'ambito dell' IT Audit è prevista anche la verifica dell'effettiva esecuzione del controllo? In altre parole, si dovrà verificare che il controllo sia effettivamente eseguito raccogliendo le opportune evidenze su base campionaria, svolgendo un test di efficacia operativa?

Risposta

Come riportato nel Capitolato Tecnico, pag. 19, il Fornitore dovrà effettuare le attività di test del disegno e dell'implementazione dei controlli. Si richiede al Fornitore, quindi, di verificare l'adeguatezza del design del controllo e la sua effettiva implementazione; non è richiesta al Fornitore l'esecuzione dell'attività di verifica dell'efficacia operativa dei controlli.

37) Domanda

LOTTO 2: ai fini di una migliore stima degli impegni, è possibile avere una descrizione, anche approssimativa, per gruppi o percentuale rispetto al totale, delle applicazioni (85 interne + 35 esposte su internet) previste nel perimetro dei ICT Security Assessment in termini di tipologia/dimensione?

Risposta

Le applicazioni interne riguardano prevalentemente le attività istituzionali (gestione dei premi, delle prestazioni, dell'area medica, ecc) e strumentali (portali, HR, contabilità, ecc) dell'Istituto. Quelle esterne sono tipicamente i servizi messi a disposizione dei clienti per il self-service del rapporto con INAIL, per le denunce, per la consultazione delle pratiche, ecc. In entrambi i casi si tratta di applicazioni scritte in JAVA. Maggiori dettagli, utili alle verifiche, verranno forniti all'aggiudicatario della gara.

38) Domanda

In merito a quanto riportato nell'Allegato 1 - Capitolato tecnico, par 3.2.3.1, pag 34 - "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",
Si richiedono dettagli circa numerosità e tipologia di policy e linee guida da sottoporre ad audit.

Risposta

Come indicato a pag 29 del capitolato tecnico (allegato 5) INAIL dispone al momento di circa 30 linee guida/best practice di sicurezza ICT che riguardano tutti gli adempimenti normativi in ambito sicurezza e le principali raccomandazioni relative alla sicurezza organizzativa e logica.

39) Domanda

Con riferimento all'Allegato 1 - Capitolato tecnico, par 3.2.3.1, pag 34 - "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".
Si richiede di indicare la forma in cui saranno rese disponibili le azioni correttive dei precedenti audit.

Risposta

I risultati della precedente campagna di controllo, saranno resi disponibili in formato elettronico.

40) Domanda

Con riferimento all'Allegato 1 - Capitolato tecnico, par 3.2.3.1, pag 34 - "L'aggiudicatario sarà tenuto a controllare, con frequenza semestrale, l'effettiva attuazione delle policy, delle linee guida e degli standard di sicurezza. Si richiede di confermare la disponibilità di checklist e verbali di precedenti audit.

Risposta

L'Istituto renderà disponibili al Fornitore i soli risultati della precedente campagna di controllo, ovvero le azioni correttive ed il relativo piano di attuazione.

41) Domanda

Con riferimento all'Allegato 1 - Capitolato tecnico, par 3.2.3.2, pag 35 -"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...",
Si richiedono dati dimensionali circa la numerosità degli amministratori e dei sistemi che sono impiegati in trattamenti di dati personali.

Risposta

Attualmente, gli amministratori di sistema che sono impiegati in trattamenti di dati personali, sono 140.

42) Domanda

Con riferimento all'Allegato 1 - Capitolato tecnico, par 3.2.3.2, pag 35 -"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...".
Si richiedono dettagli circa le modalità in cui sono rese disponibili le informazioni relative agli ambiti di impiego degli ads ed i relativi carichi di lavoro.

Risposta

Come da Capitolato Tecnico, pag. 35, sarà cura del Fornitore proporre la metodologia per l'esecuzione delle attività relative all'analisi delle attività degli amministratori di sistema. L'Istituto, così come indicato a pag. 36 del Capitolato Tecnico, renderà disponibile al Fornitore 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. Sarà inoltre fornito un elenco nominativo di tutti gli ADS e i relativi ambiti di operatività.

43) Domanda

Con riferimento all'Allegato 1 - Capitolato tecnico, par 3.2.3.2, pag 35 -"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'.
Si richiedono dettagli circa le modalità in cui sono evidenziate le tipologie di dati al cui trattamento partecipa un determinato elemento tecnico (server, db etc).

Risposta

Come premessa va detto che il sistema informativo INAIL prevede una distribuzione pressoché omogenea dei dati personali e sensibili sui vari sistemi che rende poco probabile la necessità di differenziare i controlli.

Tuttavia INAIL metterà a disposizione una mappatura che associa dati-database e una mappatura database-sistemi. Qualora queste informazioni non fossero sufficienti a categorizzare i sistemi gestiti da un amministratore si assegnerà a tali sistemi il livello di criticità più alto previsto dalla classificazione.

44) Domanda

Con riferimento all'Allegato 1 - Capitolato tecnico, par 4.1, pag 34 -"Richiesta al Fornitore di procedere alla stima dei tempi, dei costi e del mix di risorse necessari per il relativo intervento del singolo servizio".
Si richiede di indicare il rapporto tra le richieste ed il piano di lavoro.

Risposta

Le attività di cui alla tabella riportata al par. 4.1 del Capitolato Tecnico, pag. 54, rappresentano le milestone che delimitano le fasi del ciclo di vita di ogni singolo intervento progettuale, formalizzandone i vari passi. Il piano di lavoro farà riferimento alle attività specifiche di ogni singolo intervento progettuale, in funzione della metodologia proposta dall'aggiudicatario in fase di offerta e di quanto concordato con l'Amministrazione.

45) Domanda

Con riferimento all'Allegato 2 - Offerta tecnica Lotto 2, pag 5 - "MIGLIORAMENTO DEI REQUISITI MINIMI PREVISTI", Sarà valutato positivamente il possesso dl eventuali certificazioni indipendenti sulla sicurezza erogate da istituzioni alternative ad ISACA ed ISECOM?

Risposta

Sarà valutato positivamente il possesso, da parte dei vari profili previsti, delle sole certificazioni di cui ai paragrafi 3.5 e 3.6.

46) Domanda

Con riferimento all'Allegato 2 - Offerta tecnica Lotto 2, pag 5 - "MIGLIORAMENTO DEI REQUISITI MINIMI PREVISTI PER IL PROFILO DI SECURITY MANAGER".
Si può considerare la certificazione PMP equivalente alla Prince2?

Risposta

No, si veda la risposta alla domanda n. 5.

47) Domanda

Con riferimento all'Allegato 2 - Offerta tecnica Lotto 2, pag 5 - "MIGLIORAMENTO DEI REQUISITI MINIMI PREVISTI PER IL PROFILO DI SECURITY ANALYST SENIOR".
SI possono considerare le certificazioni GIAC GPEN o_GWAPT equivalenti alla OPST richiesta?

Risposta

No, si veda la risposta alla domanda n. 45.

48) Domanda

Con riferimento all'Allegato 4 - Condizioni speciali, art. 10 S comma 2: … L'impresa si impegna a consegnare i curricula, le certificazioni dichiarate in sede di offerta e l'ulteriore documentazione indicata nel Capitolato Tecnico delle risorse e delle figure professionali impegnate nell'esecuzione del contratto entro 10 (dieci) giorni lavorativi dalla stipula ....,
Si chiede di confermare che non esistono vincoli sulla data di ottenimento della certificazione, purché valida all'atto della presentazione entro 10 giorni dalla stipula del contratto.

Risposta

Si conferma che, per entrambi i Lotti, con la presentazione dell'offerta il concorrente si impegna a garantire alla Committente il possesso in capo alle risorse professionali impegnate nell'appalto dei requisiti minimi professionali (incluse le certificazioni) previsti nel Capitolato tecnico e dei requisiti migliorativi (incluse le certificazioni) previsti nel Disciplinare ed idonei al conseguimento del punteggio tecnico, eventualmente offerti, che possono essere conseguiti fino al momento della consegna dei curricula.

49) Domanda

In riferimento al profilo di Security Manager in cui si richiede "Laureato con anzianità lavorativa maggiore di 10 anni, da computarsi successivamente alla data di conseguimento del diploma di laurea, di cui almeno 3 anni di provata esperienza nella specifica funzione" si richiede se il requisito di possesso di Laurea può essere ritenuto equivalente ad una risorsa in possesso di Diploma di Maturità con esperienza lavorativa superiore a 20 anni.

Risposta

Si veda l'Errata corrige N. 3.

50) Domanda

Supporto tecnico-metodologico alle attività di Audit IT. 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;
Allegato 5 paragrafo 3.1.3.1. E' richiesta anche una stima del rischio con valutazione puramente quantitativa, ovvero espressa direttamente in termini, ad esempio, di impatto economico?

Risposta

Come indicato nel Capitolato Tecnico, la metodologia proposta dal Fornitore dovrà prevedere una valutazione sia qualitativa che quantitativa del rischio.

51) Domanda

Supporto tecnico-metodologico alle attività di Audit IT. 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. Allegato 5 paragrafo 3.1.3.1. E' possibile proporre l'uso di altri tools di analisi del rischio differenti dagli strumenti di office automation?

Risposta

No, gli strumenti a supporto delle attività saranno identificati e resi disponibili dall'Istituto.

52) Domanda

Controllo dell'efficacia delle misure di sicurezza IT . 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. Allegato paragrafo 5 3.2.3.1. E' possibile avere una quantificazione approssimativa del numero di controlli di cui è necessario verificare l'attuazione, a seguito della campagna precedente?

Risposta

Si ritiene che il valore di riferimento è dato dalla somma dei controlli fatti per verificare la rispondenza alle misure minime privacy (allegato B al D.LGS 196/2003 disciplinare tecnico in materia di misure minime di sicurezza ICT) con i controlli previsti dalla ISO/IEC 27001 (limitatamente a quelli pertinenti).

53) Domanda

Security Assessment. Assessment delle misure di sicurezza infrastrutturali: si richiede di dettagliare il significato della richiesta; se possibile con esempi.
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.

Allegato 5 paragrafo 3.2.3.3.3. E' possibile avere la quantità di sistemi e tipologia di essi ? es: IPS Tippingpoint, FW Checkpoint etc,…

Risposta

Il perimetro della fornitura è descritto nel par. 3.2.2 dell'Allegato 5 – Capitolato tecnico.

La documentazione relativa a tutti gli apparati di sicurezza attivi sulla rete e sui sistemi, sarà messa a disposizione del fornitore aggiudicatario.

54) Domanda

Security Assessment. Tra la sorgente dell'attacco ed i sistemi oggetto delle analisi sono presenti dei sistemi di IDS/IPS? Se sono presenti sistemi di questo tipo si prega di indicare le persone di riferimento da contattare in caso di comunicazioni urgenti. Se sono presenti IDS/IPS, tali sistemi devono essere attivi o non attivi durante le analisi?

Risposta

I referenti di tutti gli apparati di sicurezza attivi sulla rete e sui sistemi, saranno indicati al fornitore aggiudicatario e ogni qualvolta necessario, erogheranno il supporto necessario al security assessment. In genere i sistemi di sicurezza devono essere attivi durante i security assessment.

55) Domanda

Security Assessment. Il cliente vuole essere immediatamente informato relativamente all'individuazione di vulnerabilità con impatti molto elevati?

Risposta

SI. Qualora la vulnerabilità riscontrata comportasse un elevato rischio di sicurezza per l'infrastruttura IT, od una sua componente, è necessario che il fornitore informi immediatamente l'Istituto indicando, nel contempo, le azioni correttive da porre in essere con carattere di urgenza ai fini di una sua risoluzione/riduzione.

56) Domanda

Security Assessment. Le applicazioni/servizi web da analizzare sono protette da apparati WAF (Web Application Firewall)?

Risposta

La documentazione relativa a tutti gli apparati di sicurezza attivi sulla rete e sui sistemi, sarà messa a disposizione del fornitore aggiudicatario.

57) Domanda

ICT Security Assessment. Il fornitore 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. Allegato 5, pag. 37 paragrafo 3.2.3.3.

Risposta

Non è chiara la domanda.

58) Domanda

ICT Security Assessment. 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. Allegato 5, pag. 39 paragrafo 3.2.3.3. Che tipologia di mobile ? iOS, Android, Windows Phone

Risposta

Le app di cui è in corso lo sviluppo saranno disponibili per tutte e tre le tipologie.

59) Domanda

ICT Security Assessment. Identificazione di eventuali utenze con credenziali (username/password) facilmente deducibili. Allegato 5, pag. 39 paragrafo 3.2.3.3.1 . Con identificazione si intende un processo di password / id guessing. In queste situazione e' possibile che si verifichi il blocco dell'utenza. E' possibile avere dettagli aggiuntivi ?

Risposta

Questo tipo di controllo dovrà essere valutato di volta in volta in base ai possibili rischi di blocco citati ed alle effettive necessità. Il fornitore deve essere comunque dotato degli strumenti necessari per poterlo eseguire una volta che lo si è concordato.

60) Domanda

ICT Security Assessment. 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.
Allegato 5, pag. 43 paragrafo 3.2.3.3.2. Capitolo: VA e PT su sistemi e applicazioni presenti sulle reti private.
E' possibile avere il numero indicativo di AP e SSID ? E' possibile avere la distribuzione per sede ?

Risposta

Attualmente sono stati istallati, sulle quattro diverse sedi centrali di INAIL (tutte collocate in Roma) 21 AP, 11 AP, 7 AP e 0 AP. Ogni AP contiene 3 SSID.

Dott. Domenico Casalino
(L'Amministratore Delegato)