- **RISPOSTA AI CHIARIMENTI PERVENUTI AL 21/01/2026**

Procedura aperta per l'affidamento del Servizio di supporto al mantenimento della certificazione ISO/IEC 27001:2022 e ISO/IEC 20017:2015 relativa al Sistema di Gestione della Sicurezza delle Informazioni e per la formazione per il triennio 2026-2028 – CIG B8D98BB7B5

Chiarimenti – 1 del 15.01.2026

D. Con la richiesta di "Supporto all'attività di Vulnerability Assessment/Penetration Test (VA/PT) da parte di fornitore individuato" si chiede quali sono le attività di supporto richieste all'Aggiudicatario? In particolare, è corretto intendere che non è richiesto all'Aggiudicatario di effettuare in prima persona tale attività di VA/PT ma eventualmente un affiancamento nella gestione e definizione dei piani di VA/PT e relativa analisi dei risultati emersi?

R. Si, non è richiesta l'esecuzione dell'attività, ma il supporto;

……..

D. Con la richiesta di "Progettazione degli eventi formativi attraverso l'uso di una piattaforma di formazione on-line, messa a disposizione dell'aggiudicatario" si intende che tale piattaforma verrà fornita dalla Stazione Appaltante all'Aggiudicatario? Col termine "piattaforma" si intende uno strumento web di e-learning (formazione asincrona) o altro strumento telematico come ad esempio corsi mediante strumenti remoti come Teams, Zoom con la possibilità di registrare il corso per usi futuri?

R. No, la piattaforma dovrà essere messa a disposizione dall'Aggiudicatario in modalità asincrona;

……..

D. In merito alla richiesta di certificazione per i componenti del gruppo di lavoro, viene richiesto che "tutti i componenti del gruppo di lavoro dovranno essere in possesso della certificazione Lead Auditor ISO/IEC 27001:2022". Sono da ritenersi equipollenti anche certificazioni del tipo ISO/IEC 27001:2022 Lead Auditor Transition Training Course.

R. No, solo come aggiornamento di una qualifica già posseduta su una versione precedente, ossia per chi è già in possesso della certificazione Lead Auditor ISO/IEC 27001:2013, al fine di mantenere la qualifica di Lead Auditor ISO 27001.

……..

Chiarimenti – 2 del 19.01.2026

D. Audit interni / audit di terza parte: numerosità e sedi Riferimento: Disciplinare Tecnico, Art. 2, lett. a) (supporto ad audit interni e di eventuali terze parti con presenza presso le sedi di Acquedotto Lucano); Art. 9 (Audit e ISO 19011).

Quesito: Si richiede di indicare, per ciascuna annualità (2026, 2027, 2028), il numero stimato di:

(i) audit interni con presenza presso sedi di Acquedotto Lucano; (ii) audit di terza parte (ente di certificazione) con presenza presso sedi di Acquedotto Lucano. Si richiede inoltre di specificare quante e quali sedi potranno essere coinvolte e se alcune fasi. (es. interviste/document review) possano essere svolte da remoto, indicando eventuali vincoli

R. Basandosi sui dati storici, vengono effettuati:

a) due audit interni all'anno in presenza presso la sede di Potenza per 5 giornate complessive. Gli audit interni sono preceduti dalla preparazione in remoto per un numero di giornate dipendenti dalla complessità.

b) un audit di terza parte per il rinnovo/conferma della Certificazione, in media di cinque giorni, presso la sede di Potenza e di Matera da parte dell'Ente di certificazione.

……..

D. Supporto VA/PT svolto da fornitore terzo: perimetro attività e deliverable Riferimento: Disciplinare Tecnico, Art. 1 (servizi richiesti: supporto VA/PT) e Art. 2 (supporto al VA/PT svolto da fornitore terzo).

Quesito: Considerato che il VA/PT è svolto da un fornitore terzo a cura e spese di Acquedotto Lucano, si richiede di specificare in modo puntuale il perimetro delle attività richieste all'aggiudicatario, si chiede di confermare:

• quale sia il perimetro preciso del supporto richiesto (es. sola analisi dei report, supporto alla remediation, partecipazione alla pianificazione tecnica);

• che il supporto includa l'analisi dei report, e la gestione delle evidenze ai soli fini ISO 27001/27017 e il conseguente raccordo con il processo di risk treatment;

R. L'aggiudicatario non svolge attività tecniche di Vulnerability Assessment e Penetration Test, ma fornisce supporto consulenziale e metodologico che comprende, a titolo esemplificativo, l'analisi dei report VA/PT, con riferimento alla classificazione delle vulnerabilità, alla valutazione degli impatti su riservatezza, integrità e disponibilità e alla coerenza con il contesto ICT e di rischio aziendale, nonché il supporto alla gestione delle evidenze ai fini della conformità alle norme ISO/IEC 27001 e ISO/IEC 27017, inclusa la tracciabilità delle vulnerabilità, la correlazione con i controlli applicabili dell'Annex A, che definisce l'insieme dei controlli di sicurezza di riferimento per il Sistema di Gestione della Sicurezza delle Informazioni, il raccordo con il processo di Risk Management, il supporto all'aggiornamento del risk assessment e del risk treatment plan e il supporto alla remediation, limitatamente alla verifica documentale delle azioni correttive proposte e alla validazione formale dell'avvenuta presa in carico del rischio.

……..

D. Audit di seconda parte (n. 15): ripartizione, durata e modalità Riferimento: Disciplinare Tecnico, Art. 2, lett. a) (conduzione di audit di seconda parte; n. 15 audit).

Quesito: Si richiede conferma che il numero di audit di seconda parte sia pari a n. 15 complessivi nel triennio (e non per singola annualità). In caso di conferma, si richiede di indicare:

• la ripartizione indicativa per annualità;

• la durata indicativa per audit (giorni/uomo);

R. Si stima un numero di cinque verifiche/anno della durata di una giornata ciascuna.

……..

D. Formazione: numero utenti, profili e requisiti minimi del percorso

Riferimento: Disciplinare Tecnico, Art. 2, lett. b) (formazione erogata su piattaforma e-learning; accesso 24 mesi; attestazioni; include SGSI/ISO 27001 e GDPR).

Quesito: Si richiede di confermare la platea formativa attesa (numero stimato di utenti) e la relativa segmentazione per profilo (es. personale IT, management, personale operativo, eventuali esterni).

Inoltre, si richiede di confermare se la platea formativa coincida con le "7 risorse di Acquedotto Lucano" richiamate nel Disciplinare Tecnico (nell'ambito del SGSI.

R. La platea formativa è di circa 300 utenti per la fruizione della piattaforma online suddivisi in personale IT, dirigenti e utenti.

……..

D. Piattaforma e-learning: costo licenza a carico della Stazione Appaltante

Riferimento: Disciplinare Tecnico, Art. 2, lett. b) (piattaforma messa a disposizione) e Art. 5 (esclusioni: spese per acquisizione eventuali licenze o hardware).

Quesito: Si richiede conferma che, in coerenza con l'Art. 5, il costo di licenza/abbonamento della piattaforma e-learning sia da intendersi a carico di Acquedotto Lucano, e che pertanto tali costi siano esclusi dall'importo a base di gara.

R. La piattaforma utilizzata per l'erogazione della formazione base di cui al punto 4) è a cura dell'Aggiudicatario. La previsione secondo cui "l'acquisizione di eventuali licenze software o componenti hardware è esclusa" si riferisce esclusivamente a servizi ulteriori o diversi rispetto a quelli espressamente richiesti nel Capitolato e non si applica, pertanto, alle dotazioni necessarie per l'erogazione della formazione prevista

……..

D. Requisito servizi analoghi (EUR 50.000): definizione e cumulabilità

Riferimento: Lettera di invito, Art. 8.2, lett. A (capacità tecnica e professionale: servizi analoghi per importo non inferiore a EUR 50.000,00).

Quesito: Ai fini del requisito di cui all'Art. 8.2, lett. A, si richiede di specificare cosa debba intendersi per "servizi analoghi", chiarendo se siano considerati ammissibili esclusivamente servizi di mantenimento certificazioni ISO/IEC 27001–27017 o anche attività quali implementazione SGSI e audit interni.

R. Per servizi analoghi, sono considerati ammissibili esclusivamente servizi di mantenimento certificazioni ISO/IEC 2700127017.

……..

D. Sub-criterio 3 (Project Manager): equivalenze certificazioni

Riferimento: Lettera di invito, Art. 18 – Offerta tecnica, Sub-criterio 3 (certificazioni richieste del Responsabile di progetto: PMP; CISM; Lead Auditor ISO/IEC 27001; CISA).

Quesito: Ai fini dell'attribuzione del punteggio del Sub-criterio 3, si richiede di chiarire:

(i) se certificazioni alternative in ambito project management (es. PRINCE2) siano considerate equivalenti alla certificazione PMP;

(ii) se la certificazione Lead Auditor ISO/IEC 27001 debba essere riferita specificamente alla versione 27001:2022 oppure se siano ammesse certificazioni su versioni precedenti purché valide.

R. 1) Ai fini della presente procedura, le certificazioni richieste per il Responsabile di progetto sono esclusivamente quelle indicate nella documentazione di gara. Non sono previste certificazioni alternative o equivalenti.

R. 2) La certificazione Lead Auditor ISO/IEC 27001 è riferita alla versione 27001:2022

……..

D. Sub-criterio 4 (Gruppo di lavoro): equivalenze ITIL/COBIT

Riferimento: Lettera di invito, Art. 18 – Offerta tecnica, Sub-criterio 4 (certificazioni del Gruppo di lavoro).

Quesito: Ai fini dell'attribuzione del punteggio del Sub-criterio 4, si richiede di chiarire se siano considerate equivalenti certificazioni su versioni/edizioni successive, in particolare:

(i) ITIL 4 in alternativa a ITIL v.3;

(ii) COBIT 2019 in alternativa a COBIT 5.

R. Ai fini dell'attribuzione del punteggio previsto dal Sub-criterio 4, si chiarisce che sono considerate equivalenti le certificazioni conseguite su versioni o edizioni successive dei medesimi framework, in quanto rappresentano un'evoluzione degli standard di riferimento e ne preservano l'impianto concettuale e gli ambiti di competenza fondamentali.

……..

D. Relazione tecnica: limite 10 facciate e criteri di conteggio

Riferimento: Lettera di invito, Art. 16, lett. b) (Relazione tecnica max 10 facciate, numerate, formato e parametri di impaginazione; A3 conteggiato come 2 A4; contenuti oltre limite non valutati).

Quesito: Si richiede di chiarire se nel limite massimo di 10 facciate rientrino anche copertina/frontespizio, indice e/o eventuale presentazione aziendale, nonché se eventuali pagine di separazione tra sezioni siano computate nel limite. Si richiede inoltre conferma che l'inserimento di tabelle/figure/diagrammi sia ammesso nel rispetto dei parametri di impaginazione.

R. Si rimanda a quanto riportato nella lettera di invito all'Art. 16 Punto Lett. b) precisando che, alla luce di quanto previsto nella lettera di invito, schede, diagrammi, relazioni a corredo o quadri riassuntivi che mettano meglio in evidenza i contenuti della proposta non sono incluse nelle 10 pagine previste.

……..

D. Relazione tecnica: “schede/diagrammi/quadri riassuntivi” oltre il limite e allegati Riferimento: Lettera di invito, Art. 16, lett. b) (possibilità di presentare schede, diagrammi o quadri riassuntivi; chiarimento sul rapporto con il limite di 10 facciate).

Quesito: Si richiede di chiarire se le “schede, diagrammi o quadri riassuntivi” siano:

(i) pagine aggiuntive non soggette al limite delle 10 facciate; oppure

(ii) allegati separati ammessi ma non valutabili; oppure

(iii) comunque soggetti al limite delle 10 facciate.

Si richiede inoltre di chiarire se allegati quali CV, copie certificazioni e schede tecniche della piattaforma e-learning siano documentazione a parte (non soggetta al limite) o se debbano essere ricompresi nel limite delle 10 facciate.

R. Si rimanda a quanto riportato nella lettera di invito all’Art. 16 Punto Lett. b) precisando che, alla luce di quanto previsto nella lettera di invito, schede, diagrammi, relazioni a corredo o quadri riassuntivi che mettano meglio in evidenza i contenuti della proposta non sono incluse nelle 10 pagine previste.

……..