**UFFICIO INFORMATICA, SICUREZZA,
RETI E PROTEZIONE DEI DATI PERSONALI**
Dipartimento Funzione Pubblica

ALLEGATO "A"

CAPITOLATO SPECIALE
PER IL MANTENIMENTO E IL RINNOVO DELLA CERTIFICAZIONE ISO/IEC 27001:2022 DEL PROCESSO CRS E DEI SERVIZI SERC E RDD

1. OGGETTO DELLA PROCEDURA

La presente procedura di gara, articolata in due distinti lotti, ha per oggetto l'affidamento dei servizi necessari al mantenimento e al successivo rinnovo della certificazione del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) conforme alla norma **ISO/IEC 27001:2022**, relativamente al seguente perimetro:

- **CRS – Common Reporting Standard**;
- **SERC – Servizio Elettronico di Recapito Certificato**;
- **RDD – Registro dei Domicili Digitali**;

all'interno della IT (Information Technology) della Pubblica Amministrazione della Repubblica di San Marino.
La certificazione ISO/IEC 27001:2022 attualmente in essere è identificata dal **certificato n. 71347/A/0001/UK/It**, emesso in data **18 ottobre 2025**, con scadenza **12 ottobre 2028**, relativo al **4° ciclo di certificazione**.

Il certificato indica quale riferimento per la Dichiarazione di Applicabilità la:
Statement of Applicability (SoA) Rev. 4 del 31/01/2025.
L'attuale certificazione rappresenta la prosecuzione di un percorso iniziato nell'anno 2016, quando la certificazione comprendeva inizialmente il solo processo CRS, e successivamente esteso al SERC e al RDD.

Ai fini della formulazione dell'offerta economica, i partecipanti dovranno tenere conto dell'intero ciclo triennale previsto per il mantenimento e il rinnovo della certificazione ISO/IEC 27001, articolato come segue:

- **Anno 2026:** attività di mantenimento della certificazione;
- **Anno 2027:** attività di mantenimento della certificazione;
- **Anno 2028:** attività di mantenimento e riemissione/rinnovo della certificazione.

L'offerta economica dovrà pertanto riportare distintamente il **costo previsto per l'anno 2026** e il **costo riferito al triennio 2026-2028**, con evidenza dei singoli importi annuali.
In sede di valutazione delle offerte, **sarà data priorità all'offerta formulata per l'intero periodo 2026-2028**, secondo le condizioni economiche e contrattuali risultanti dalla procedura di gara.

Si precisa che l'eventuale affidamento delle attività relative agli anni 2027 e 2028 è subordinato alla preventiva **autorizzazione della spesa triennale** da parte dell'Amministrazione.

In caso di mancata approvazione dell'autorizzazione alla spesa triennale, si procederà, unicamente per l'annualità 2026 per questo verranno richieste offerte distinte, solo 2026 oppure 2026, 2027, 2028.

La procedura è articolata in due lotti:

LOTTO 1
Servizi specialistici di supporto al Sistema di Gestione per la Sicurezza delle Informazioni, aggiornamento della documentazione, gestione del rischio, audit interno, supporto all'audit di certificazione e attività di Vulnerability Assessment e Penetration Test.

LOTTO 2
Servizi dell'Organismo di Certificazione finalizzati al mantenimento della certificazione mediante audit di sorveglianza negli anni 2026 e 2027 e al rinnovo della certificazione nell'anno 2028.

I due lotti sono funzionalmente complementari, ma dovranno essere affidati a soggetti distinti al fine di garantire l'indipendenza dell'attività di certificazione rispetto alle attività di supporto.

2. PERIMETRO DELLA CERTIFICAZIONE

Il perimetro della certificazione è quello riportato nel certificato ISO/IEC 27001:2022 n. **71347/A/0001/UK/It**:

"Sicurezza delle informazioni dei servizi: CRS (Common Reporting Standard), SERC (Servizio Elettronico di Recapito Certificato), RDD (Registro dei Domicili Digitali), all'interno della IT (Information Technology) della Pubblica Amministrazione della Repubblica di San Marino."

Le attività oggetto del presente capitolato dovranno essere riferite a tale perimetro, salvo eventuali successive variazioni formalmente concordate dalla Stazione Appaltante nell'ambito del Sistema di Gestione per la Sicurezza delle Informazioni.

L'Impresa Aggiudicataria del Lotto 1 dovrà tenere conto, nello svolgimento delle proprie attività, della documentazione vigente del SGSI e, in particolare, della **Statement of Applicability Rev. 4 del 31/01/2025**.

3. FINALITÀ DELL'APPALTO

La finalità della presente procedura è garantire la continuità e il miglioramento del Sistema di Gestione per la Sicurezza delle Informazioni e della relativa certificazione ISO/IEC 27001:2022 attraverso:

1. Il mantenimento del SGSI esistente;
2. L'aggiornamento della documentazione e dei processi;
3. Il monitoraggio e l'aggiornamento della valutazione dei rischi;
4. La verifica dell'attuazione dei controlli di sicurezza;
5. L'aggiornamento della Statement of Applicability ove necessario;
6. Lo svolgimento degli audit interni;
7. L'individuazione e la gestione delle eventuali non conformità;
8. L'esecuzione di attività di Vulnerability Assessment e Penetration Test;
9. La preparazione della Stazione Appaltante agli audit dell'Organismo di Certificazione;
10. Il mantenimento della certificazione negli anni 2026 e 2027;
11. La preparazione e il supporto alle attività di rinnovo della certificazione nell'anno 2028;
12. L'aggiornamento del personale.

4. RIFERIMENTI NORMATIVI E TECNICI

Le attività dovranno essere svolte in conformità alla normativa vigente e, per quanto applicabile, ai seguenti riferimenti:

- **ISO/IEC 27001:2022 – Sicurezza delle informazioni, cybersecurity e protezione della privacy — Sistemi di gestione della sicurezza delle informazioni — Requisiti**
- **ISO/IEC 27002:2022 – Sicurezza delle informazioni, cybersecurity e protezione della privacy — Controlli di sicurezza delle informazioni**
- Ulteriori standard ISO/IEC applicabili alle attività oggetto del servizio;
- Normativa della Repubblica di San Marino applicabile alla sicurezza delle informazioni;
- Normativa applicabile alla protezione dei dati personali;
- Normativa applicabile ai servizi digitali e ai servizi elettronici della Pubblica Amministrazione;
- Legge n. 171/2018 e successive modifiche, relativa alla protezione dei dati personali: Protezione delle persone fisiche con riguardo al trattamento dei dati personali
- Decreto Delegato 30 gennaio 2020 n. 9; Modifiche al Decreto 8 novembre 2005 n.156 e disposizioni sull'utilizzo di servizi elettronici di recapito certificato e di posta elettronica certificata
- Regolamento 22 novembre 2018 n. 7: Regolamento per l'utilizzo del Registro Pubblico dei Domicili Digitali
- Decreto Delegato 26 luglio 2018 n. 92: Modifiche al Decreto Delegato 11 aprile 2016 n.46 - Disposizioni per l'utilizzo di servizi elettronici di recapito certificato qualificato

- Decreto Delegato 15 giugno 2018 n. 65: Modifiche al Decreto Delegato 11 aprile 2016 n.46 - Disposizioni per l'utilizzo di servizi elettronici di recapito certificato qualificato
- Legge 23 agosto 2016 n. 114: Disciplina dei Reati Informatici
- Decreto Delegato 11 aprile 2016 n. 46: Disposizioni per l'utilizzo di servizi elettronici di recapito certificato qualificato
- Legge 29 maggio 2013 n. 58: Legge sull'uso delle comunicazioni elettroniche e dell'E-Commerce
- Regolamento 30 dicembre 2015 n. 20: Regolamento tecnico per la protezione dei dati personali in applicazione dello scambio di informazione in materia fiscale
- Decreto 8 novembre 2005 n. 156: Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici
- Legge 20 luglio 2005 n. 115: Legge sul documento informatico e la firma elettronica

L'elenco dei riferimenti normativi dovrà essere verificato e aggiornato alla data di pubblicazione della procedura e durante l'esecuzione del contratto, per quanto applicabile.

5. DURATA E ARTICOLAZIONE TEMPORALE

La certificazione attualmente in essere ha:

- **Data di emissione:** 18 ottobre 2025;
- **Data di scadenza:** 12 ottobre 2028;
- **Ciclo di certificazione:** 4.

La presente procedura è pertanto finalizzata a garantire la continuità della certificazione durante l'intero periodo di validità e il successivo rinnovo.

Le attività saranno articolate come segue:

Annualità	Lotto 1	Lotto 2
2026	Mantenimento SGSI, aggiornamento documentazione, audit interno, VA/PT, preparazione e supporto all'audit	Audit di sorveglianza
2027	Mantenimento SGSI, aggiornamento documentazione, audit interno, VA/PT, preparazione e supporto all'audit	Audit di sorveglianza
2028	Preparazione al rinnovo, audit interno, VA/PT e supporto alla ricertificazione	Audit di rinnovo

Le attività relative all'annualità 2026 dovranno essere pianificate in modo da consentire il completamento delle attività preparatorie entro la data prevista per l'audit dell'Organismo di Certificazione.

LOTTO 1

6. OGGETTO DEL LOTTO 1

Il Lotto 1 comprende le attività di supporto specialistico necessarie al mantenimento e al miglioramento del Sistema di Gestione per la Sicurezza delle Informazioni conforme alla ISO/IEC 27001:2022.
Sono comprese nel Lotto 1:

- Analisi dello stato del SGSI;
- Gap Analysis;
- Aggiornamento della documentazione;
- Supporto alla gestione del rischio;
- Aggiornamento della Statement of Applicability;
- Definizione e monitoraggio degli obiettivi;
- Audit interno;
- Gestione e follow-up delle azioni correttive;

- Preparazione agli audit dell'Organismo di Certificazione;
- Supporto durante le giornate di audit;
- Vulnerability Assessment;
- Penetration Test;
- Reportistica tecnica ed executive;
- Supporto alla definizione del piano di remediation;
- Eventuale attività di retest.

L'Impresa Aggiudicataria dovrà operare come soggetto di supporto e indirizzo della Stazione Appaltante.
L'Impresa Aggiudicataria del Lotto 1 **non svolgerà attività di certificazione** e non potrà assumere decisioni relative al rilascio, mantenimento, rinnovo, sospensione o revoca della certificazione.

7. GAP ANALYSIS DEL SISTEMA DI GESTIONE

All'avvio del servizio l'Impresa Aggiudicataria dovrà effettuare una Gap Analysis del SGSI esistente.
La verifica dovrà comprendere almeno:

- Analisi del contesto dell'organizzazione;
- Verifica dello scope;
- Analisi delle parti interessate;
- Verifica delle politiche di sicurezza;
- Verifica della metodologia di valutazione del rischio;
- Analisi del Risk Assessment vigente;
- Analisi del Risk Treatment Plan;
- Verifica della Statement of Applicability Rev. 4 del 31/01/2025;
- Verifica dell'attuazione dei controlli applicabili;
- Analisi degli audit precedenti;
- Analisi delle eventuali non conformità;
- Analisi delle osservazioni;
- Verifica dello stato delle azioni correttive;
- Verifica della documentazione del SGSI;
- Individuazione delle eventuali aree di miglioramento.

Al termine dovrà essere prodotto un **Gap Analysis Report**.

8. AGGIORNAMENTO DEL SGSI E DELLA DOCUMENTAZIONE

L'Impresa Aggiudicataria dovrà supportare la Stazione Appaltante nell'aggiornamento e nel miglioramento continuo del SGSI.
Le attività potranno comprendere:

- Aggiornamento delle politiche di sicurezza;
- Aggiornamento dell'analisi del contesto;
- Aggiornamento dello scope;
- Aggiornamento delle procedure;
- Aggiornamento delle istruzioni operative;
- Aggiornamento delle metodologie;
- Aggiornamento della documentazione relativa ai controlli;
- Aggiornamento della documentazione relativa alla gestione degli incidenti;
- Aggiornamento della documentazione relativa alla continuità operativa, ove ricompresa nel SGSI;
- Aggiornamento della documentazione relativa alla gestione degli accessi;
- Aggiornamento della documentazione relativa agli asset;
- Supporto nella predisposizione delle evidenze richieste dagli audit.

L'attività dovrà essere finalizzata al mantenimento dell'effettiva conformità del SGSI e non alla sola produzione o revisione formale dei documenti.

9. ANALISI E GESTIONE DEI RISCHI

L'Impresa Aggiudicataria dovrà supportare la Stazione Appaltante nell'aggiornamento della valutazione dei rischi per la sicurezza delle informazioni.
L'attività dovrà comprendere, ove necessario:

- Identificazione degli asset;
- Identificazione delle minacce;
- Identificazione delle vulnerabilità;
- Valutazione della probabilità;
- Valutazione dell'impatto;
- Determinazione del livello di rischio;
- Individuazione delle misure di trattamento;
- Valutazione del rischio residuo;
- Aggiornamento del Risk Treatment Plan.

Dovranno essere evidenziate le variazioni significative rispetto alla precedente valutazione.

10. STATEMENT OF APPLICABILITY

L'Impresa Aggiudicataria dovrà verificare periodicamente la coerenza della **Statement of Applicability Rev. 4 del 31/01/2025** con:

- Il perimetro della certificazione;
- Il Risk Assessment;
- Il Risk Treatment Plan;
- L'organizzazione;
- L'infrastruttura tecnologica;
- I servizi erogati;
- I controlli effettivamente implementati.

Qualora necessario, l'Impresa Aggiudicataria dovrà predisporre una proposta di aggiornamento della SoA. Ogni variazione dovrà essere sottoposta all'approvazione della Stazione Appaltante.

11. OBIETTIVI DEL SGSI

L'Impresa Aggiudicataria dovrà supportare la Stazione Appaltante nella definizione, aggiornamento e monitoraggio degli obiettivi del SGSI.
Per ciascun obiettivo dovranno essere individuati, ove applicabili:

- Risultato atteso;
- Indicatore;
- Valore obiettivo;
- Responsabile;
- Tempistica;
- Modalità di verifica;
- Evidenze.

12. AUDIT INTERNO

L'Impresa Aggiudicataria dovrà effettuare almeno un audit interno del SGSI per ciascuna annualità prevista dal contratto.
L'audit dovrà comprendere:

- Predisposizione del piano di audit;
- Definizione degli obiettivi;
- Definizione del campo dell'audit;
- Analisi documentale;
- Interviste;
- Verifica delle evidenze;
- Verifica dell'attuazione dei processi;
- Verifica dei controlli;

- Individuazione delle non conformità;
- Individuazione delle osservazioni;
- Individuazione delle opportunità di miglioramento;
- Predisposizione del rapporto di audit;
- Proposta delle azioni correttive;
- Follow-up delle azioni.

Il personale incaricato dell'audit dovrà possedere adeguata esperienza e competenza e dovrà garantire obiettività nello svolgimento delle verifiche.

13. SUPPORTO ALL'ORGANISMO DI CERTIFICAZIONE

L'Impresa Aggiudicataria dovrà supportare la Stazione Appaltante durante le attività di audit svolte dall'Organismo di Certificazione nell'ambito del Lotto 2.

Il supporto potrà comprendere:

- Preparazione dell'audit;
- Verifica della disponibilità delle evidenze;
- Coordinamento delle attività;
- Assistenza durante le giornate di audit;
- Supporto nella gestione delle richieste documentali;
- Supporto nell'analisi delle eventuali osservazioni;
- Supporto nella gestione delle eventuali non conformità;
- Supporto nella predisposizione delle azioni correttive.

14. VULNERABILITY ASSESSMENT E PENETRATION TEST

Nell'ambito del Lotto 1 dovrà essere effettuata un'attività di sicurezza informatica finalizzata a verificare il livello di esposizione e vulnerabilità dell'infrastruttura della Stazione Appaltante.
L'attività dovrà comprendere:

- **Vulnerability Assessment**;
- **Penetration Test**.

I test dovranno essere effettuati:

- In modalità **Black Box** sul perimetro esposto verso Internet;
- In modalità **Grey Box** sulle reti interne individuate dalla Stazione Appaltante.

Le attività di Penetration Test dovranno essere preventivamente autorizzate.

15. PERIMETRO INDICATIVO DEL VA/PT

Ai fini della formulazione dell'offerta, il concorrente dovrà considerare indicativamente il seguente perimetro:

Elemento	Quantità indicativa
IP utilizzati da server HTTP/HTTPS	18
IP presenti in DMZ	58
PC nel dominio	1.175
Utenti registrati a dominio	4.130
Gruppi registrati a dominio	1.293

I quantitativi indicati sono da considerarsi come riferimento per la valutazione della complessità dell'attività.
Il perimetro definitivo e gli indirizzi IP da sottoporre a test saranno comunicati all'Impresa Aggiudicataria dalla Stazione Appaltante nell'ambito della fase di pianificazione.

16. PIANIFICAZIONE E REGOLE DI INGAGGIO

Prima dell'avvio dei test dovrà essere predisposto un documento di **Rules of Engagement**, concordato e approvato dalla Stazione Appaltante.
Il documento dovrà indicare almeno:

- Sistemi oggetto del test;
- Indirizzi IP;
- Hostname;
- Applicazioni;
- Modalità di test;
- Finestre temporali;
- Strumenti utilizzabili;
- Attività consentite;
- Attività vietate;
- Referenti;
- Modalità di comunicazione;
- Procedure di emergenza;
- Modalità di sospensione dei test;
- Gestione delle evidenze.

Nessuna attività di Penetration Test potrà essere effettuata al di fuori del perimetro autorizzato.

17. ATTIVITÀ DI PREANALISI

L'Impresa Aggiudicataria dovrà svolgere almeno:

- Definizione del team;
- Definizione degli obiettivi;
- Definizione dello scope;
- Analisi delle tecnologie;
- Network footprinting;
- Definizione degli strumenti;
- Predisposizione dei sistemi di analisi;
- Definizione della metodologia.

18. ATTIVITÀ DI ENUMERATION

Dovranno essere effettuate, ove applicabili:

- Enumerazione dei sistemi;
- Enumerazione degli indirizzi IP;
- Information gathering passivo;
- Information gathering attivo, previa autorizzazione;
- Identificazione dei protocolli;
- Identificazione dei servizi;
- Analisi dello stato dei sistemi;
- Identificazione delle tecnologie.

19. VULNERABILITY ASSESSMENT

L'attività dovrà comprendere:

- Scansioni automatiche;
- Analisi mediante strumenti specifici;
- Analisi manuale;
- Verifica delle vulnerabilità dei sistemi;
- Verifica delle vulnerabilità delle applicazioni;
- Verifica delle configurazioni;
- Verifica dei servizi esposti;

- Validazione manuale dei risultati.

Le scansioni dovranno essere configurate in modo da ridurre al minimo il rischio di impatto sui sistemi in produzione.

20. PENETRATION TEST

Il Penetration Test potrà comprendere, previa autorizzazione:

- Attacchi automatici;
- Attacchi manuali;
- Exploitation controllata delle vulnerabilità;
- Client-side attacks;
- Web application attacks;
- Password attacks;
- Privilege escalation;
- Network attacks;
- Port forwarding/redirection;
- Tunneling;
- Social engineering.

Sono espressamente esclusi:

- Denial of Service;
- Stress test;
- Attività finalizzate a provocare indisponibilità dei servizi;
- Cancellazione o alterazione non autorizzata dei dati;
- Propagazione di malware;
- Modifiche permanenti ai sistemi.

Eventuali attività particolarmente invasive dovranno essere oggetto di specifica autorizzazione scritta.

21. GESTIONE DELLE VULNERABILITÀ CRITICHE

Qualora venga individuata una vulnerabilità critica o una condizione di rischio immediato e significativo, L'Impresa Aggiudicataria dovrà informare tempestivamente la Stazione Appaltante senza attendere la conclusione dell'attività.

La segnalazione dovrà contenere almeno:

- Asset interessato;
- Vulnerabilità;
- Livello di criticità;
- Impatto potenziale;
- Indicazioni per la mitigazione immediata.

22. REPORTISTICA VA/PT

Al termine delle attività dovranno essere prodotti almeno:

Report tecnico

Il report dovrà contenere:

- Perimetro analizzato;
- Metodologia;
- Strumenti utilizzati;
- Periodo di esecuzione;
- Eventuali limitazioni;
- Vulnerabilità rilevate;
- Anomalie rilevate;
- Evidenze tecniche;
- Classificazione della severità;
- CVE, ove disponibile;

- CVSS, ove applicabile;
- Asset interessato;
- IP;
- Hostname;
- Descrizione;
- Impatto;
- Modalità di riproduzione;
- Eventuale exploitation effettuata;
- Presenza di exploit pubblici, ove verificabile;
- Remediation proposta;
- Priorità di intervento.

Executive Report
Dovrà contenere:

- Sintesi delle attività;
- Perimetro;
- Metodologia;
- Principali risultati;
- Distribuzione delle vulnerabilità;
- Principali rischi;
- Impatti;
- Priorità;
- Indicazioni di remediation.

Il report dovrà riferire esclusivamente le vulnerabilità e anomalie **effettivamente rilevate nell'ambito delle attività eseguite**, evidenziando le eventuali limitazioni dell'analisi.

23. PIANO DI REMEDIATION
L'Impresa Aggiudicataria dovrà supportare la Stazione Appaltante nella predisposizione di un piano di remediation.
Per ogni vulnerabilità dovranno essere indicati, ove applicabili:

- Identificativo;
- Asset;
- Severità;
- CVSS;
- Descrizione;
- Azione correttiva dettagliata;
- Priorità;
- Modalità di verifica;
- Eventuali dipendenze.

L'Impresa Aggiudicataria dovrà presentare e discutere i risultati con i referenti della Stazione Appaltante.

24. RETEST
A seguito della risoluzione delle vulnerabilità critiche e alte, la Stazione Appaltante potrà richiedere un'attività di retest.
Il retest sarà finalizzato a verificare l'effettiva risoluzione delle vulnerabilità precedentemente rilevate.
L'Impresa Aggiudicataria dovrà indicare nell'offerta il numero di giornate/uomo previste per l'eventuale retest.

25. GIORNI/UOMO E PIANO DI LAVORO
L'Impresa Aggiudicataria dovrà indicare per ciascuna attività il relativo impegno espresso in giorni/uomo.
Dovranno essere indicati almeno:

- Attività;
- Numero di giornate/uomo;
- Profilo professionale;
- Modalità di esecuzione;
- Eventuale presenza presso la Stazione Appaltante;
- Deliverable come: report di ricerca, piani di progetto, strategie o documenti di analisi.

Il piano definitivo delle attività sarà concordato con la Stazione Appaltante.

26. DELIVERABLE DEL LOTTO 1

Il Lotto 1 dovrà produrre, secondo le attività effettivamente svolte:

1. Gap Analysis Report;
2. Piano delle azioni;
3. Documentazione SGSI aggiornata;
4. Risk Assessment;
5. Risk Treatment Plan;
6. Statement of Applicability aggiornata, ove necessario;
7. Piano di audit interno;
8. Report tecnico VA/PT;
9. Executive report VA/PT;
10. Rapporto di audit interno;
11. Piano di remediation;
12. Eventuale report di retest;
13. Documentazione di supporto agli audit dell'Organismo di Certificazione.

27. ATTIVITÀ DEL LOTTO 1 – ANNUALITÀ 2026

Per l'annualità 2026 dovranno essere previste almeno:

- Gap Analysis iniziale;
- Verifica dello stato del SGSI;
- Aggiornamento della documentazione;
- Verifica e aggiornamento del Risk Assessment;
- Verifica del Risk Treatment;
- Verifica della SoA Rev. 4 del 31/01/2025;
- VA/PT;
- Audit interno;
- Predisposizione dei report;
- Supporto alla remediation;
- Preparazione all'audit di sorveglianza;
- Affiancamento durante l'audit dell'Organismo di Certificazione;
- Aggiornamento per almeno 6 ore del personale coinvolto.

Le attività dovranno essere completate in tempo utile rispetto alla data dell'audit di sorveglianza 2026 e comunque secondo il cronoprogramma concordato con la Stazione Appaltante.

28. ATTIVITÀ DEL LOTTO 1 – ANNUALITÀ 2027

Per l'annualità 2027 dovranno essere previste almeno:

- Gap Analysis iniziale;
- Verifica dello stato del SGSI;
- Aggiornamento della documentazione;
- Verifica e aggiornamento del Risk Assessment;
- Verifica del Risk Treatment;
- Verifica della SoA Rev. 4 del 31/01/2025;
- VA/PT;

REPUBBLICA DI SAN MARINO

Via 28 Luglio, 192 - 47893 Borgo Maggiore
T +378 (0549) 885150
Mail: info.informatica@pa.sm

- Audit interno;
- Predisposizione dei report;
- Supporto alla remediation;
- Preparazione all'audit di sorveglianza;
- Affiancamento durante l'audit dell'Organismo di Certificazione;
- Aggiornamento per almeno 6 ore del personale coinvolto.

Le attività dovranno essere completate in tempo utile rispetto alla data dell'audit di sorveglianza 2027 e comunque secondo il cronoprogramma concordato con la Stazione Appaltante.

29. ATTIVITÀ DEL LOTTO 1 – ANNUALITÀ 2028

Per l'annualità 2028 dovranno essere previste le attività necessarie alla preparazione del rinnovo della certificazione, comprendenti almeno:

- Aggiornamento del SGSI;
- Verifica dello scope;
- Aggiornamento del Risk Assessment;
- Aggiornamento del Risk Treatment;
- Verifica della SoA;
- VA/PT;
- Audit interno;
- Verifica delle azioni correttive;
- Preparazione alla ricertificazione;
- Supporto durante l'audit di rinnovo;
- Supporto alla gestione delle eventuali risultanze dell'audit;
- Aggiornamento per almeno 6 ore del personale coinvolto.

Le attività dovranno essere pianificate tenendo conto della **scadenza del certificato al 12 ottobre 2028**, in modo da consentire lo svolgimento tempestivo dell'iter di rinnovo.

30. OFFERTA ECONOMICA DEL LOTTO 1

L'offerta economica dovrà comprendere tutti i costi necessari allo svolgimento del servizio.

Dovranno essere indicati separatamente:

- Per la quotazione annuale:
  - Costo attività di supporto alla certificazione e VA/PT 2026;
- Per la quotazione triennale:
  - Costo attività di supporto alla certificazione e VA/PT 2026;
  - Costo attività di supporto alla certificazione e VA/PT 2027;
  - Costo attività di supporto alla certificazione e VA/PT 2028.

L'offerta economica dovrà comprendere, ove applicabili:

- Attività di pianificazione;
- Giornate di audit;
- Trasferte;
- Spese di viaggio;
- Vitto e alloggio;
- Attività di reporting;
- Attività amministrative, come previste dal Capitolato Generale pubblicato sul sito gov.sm.

LOTTO 2

31. OGGETTO DEL LOTTO 2

Il Lotto 2 riguarda esclusivamente l'attività dell'Organismo di Certificazione finalizzata al:

- Mantenimento della certificazione nell'anno 2026;
- Mantenimento della certificazione nell'anno 2027;
- Rinnovo della certificazione nell'anno 2028.

L'attività dovrà riguardare esclusivamente il perimetro certificato CRS, SERC e RDD.

32. REQUISITI DELL'ORGANISMO DI CERTIFICAZIONE

L'Organismo di Certificazione dovrà possedere i requisiti di competenza, indipendenza e accreditamento previsti per lo svolgimento delle attività di certificazione dei Sistemi di Gestione per la Sicurezza delle Informazioni secondo la ISO/IEC 27001.
La certificazione dovrà essere rilasciata nell'ambito di un sistema di accreditamento riconosciuto.

33. AUDIT DI SORVEGLIANZA 2026

L'Organismo di Certificazione dovrà effettuare l'audit di sorveglianza previsto per il primo anno del ciclo di certificazione.
L'attività dovrà comprendere tutte le verifiche previste dalle regole applicabili al ciclo di certificazione.
Dovranno essere comprese:

- Pianificazione;
- Esame della documentazione;
- Visita ispettiva;
- Interviste;
- Verifica delle evidenze;
- Verifica dell'attuazione del SGSI;
- Verifica delle eventuali azioni correttive;
- Rapporto di audit;
- Gestione delle eventuali non conformità;
- Attività conseguenti alla decisione di certificazione.

34. AUDIT DI SORVEGLIANZA 2027

L'Organismo di Certificazione dovrà effettuare il successivo audit di sorveglianza nell'anno 2027.
L'attività dovrà comprendere tutte le verifiche previste dal programma di certificazione applicabile.

35. AUDIT DI RINNOVO 2028

Nell'anno 2028 dovrà essere effettuato l'audit di rinnovo della certificazione.
L'attività dovrà essere pianificata tenendo conto della scadenza del certificato, fissata al **12 ottobre 2028**, e dovrà consentire, ove sussistano i presupposti, la prosecuzione della certificazione senza soluzione di continuità.
Il servizio dovrà comprendere tutte le attività previste dall'iter di ricertificazione, dalla pianificazione fino alla decisione finale e all'emissione del nuovo certificato.

36. OFFERTA ECONOMICA DEL LOTTO 2

L'offerta economica dovrà comprendere tutti i costi necessari allo svolgimento del servizio.
Considerato che l'attuale certificato è emesso da UKAS, qualora l'Impresa Aggiudicataria utilizzi un ente certificatore differente, nel formulare l'offerta economica dovranno essere tenuti in considerazione i costi relativi al trasferimento del certificato.

Dovranno essere indicati separatamente:

- Per la quotazione annuale:
  - Costo audit sorveglianza 2026;

- Per la quotazione triennale:
  - Costo audit di sorveglianza 2026;
  - Costo audit di sorveglianza 2027;
  - Costo audit di rinnovo 2028.

L'offerta economica dovrà comprendere, ove applicabili:

- Attività di pianificazione;
- Giornate di audit;
- Trasferte;
- Spese di viaggio;
- Vitto e alloggio;
- Attività di reporting;
- Attività amministrative, come previste dal Capitolato Generale pubblicato sul sito gov.sm;
- Emissione e gestione del certificato.

DISPOSIZIONI COMUNI PER ENTRAMBI I LOTTI

37. DIVIETO DI PARTECIPAZIONE AD ENTRAMBI I LOTTI

Considerata la complementarità delle attività e la necessità di garantire l'indipendenza dell'attività di certificazione, ciascun operatore economico potrà partecipare esclusivamente ad uno dei due lotti.
Pertanto:

- Il concorrente del Lotto 1 non potrà partecipare al Lotto 2;
- Il concorrente del Lotto 2 non potrà partecipare al Lotto 1.

Il divieto verrà applicato anche alle forme di partecipazione associata.

38. REQUISITI DELLE IMPRESE – LOTTO 1

L'Impresa che intenderà partecipare al Lotto 1 dovrà dimostrare esperienza documentabile in attività analoghe.
In particolare, dovrà essere documentata esperienza in:

- ISO/IEC 27001;
- SGSI;
- Risk assessment;
- Audit interni;
- Cybersecurity;
- Vulnerability Assessment;
- Penetration Test.

Inoltre dovrà presentare il gruppo di lavoro proposto, indicando:

- Ruolo;
- Esperienza;
- Competenze;
- Certificazioni professionali;
- Esperienza in progetti analoghi;
- Numero di anni di esperienza.

39. REQUISITI DEL LOTTO 2

L'Impresa che intenderà partecipare al Lotto 2 dovrà dimostrare:

- Possesso dell'accreditamento richiesto;
- Competenza nello schema ISO/IEC 27001;
- Esperienza nella certificazione di SGSI;

- Disponibilità di auditor qualificati;

40. RISERVATEZZA

Tutte le informazioni acquisite durante l'esecuzione del contratto dovranno essere trattate come riservate.
L'Impresa Aggiudicataria dovrà garantire che il proprio personale e gli eventuali collaboratori siano vincolati alla riservatezza.
Per le attività nel LOTTO 1 relative al VA/PT, particolare attenzione dovrà essere posta alla protezione:

- Degli indirizzi IP;
- Delle configurazioni;
- Delle vulnerabilità;
- Delle credenziali;
- Delle evidenze tecniche;
- Dei report;
- Delle informazioni relative agli utenti;
- Delle informazioni relative all'infrastruttura.

41. INTERFERENZE CON ALTRE IMPRESE

L'Impresa Appaltatrice dovrà coordinarsi con le altre imprese e con i fornitori eventualmente presenti presso la Stazione Appaltante.
Le attività dovranno essere pianificate in modo da non arrecare pregiudizio alla continuità dei servizi.
Per le attività di sicurezza informatica dovranno essere rispettate le Rules of Engagement approvate.

42. MODALITÀ DI ESECUZIONE

Il servizio dovrà essere eseguito con la massima cura, diligenza, tempestività e riservatezza, mediante l'impiego di personale qualificato e di risorse adeguate.
L'Impresa Aggiudicataria dovrà garantire la collaborazione con i referenti tecnici e organizzativi della Stazione Appaltante.
Tutte le attività accessorie e strumentali necessarie alla corretta esecuzione delle prestazioni espressamente previste dal capitolato dovranno essere ricomprese nell'offerta, purché rientranti nella natura e nell'oggetto del servizio.

43. DIRETTORE DELL'ESECUZIONE

Divenuta efficace la delibera di aggiudicazione, a seguito degli eventuali controlli previsti dalla normativa applicabile, la Stazione Appaltante nominerà il Direttore dell'Esecuzione.
Nel contratto saranno indicati il nominativo e i recapiti del Direttore dell'Esecuzione.

44. MODALITÀ DI FORMULAZIONE DELL'OFFERTA

L'offerta tecnica dovrà essere formulata secondo le modalità indicate negli atti di gara.
Per il Lotto 1, nella relazione illustrativa, dovranno possibilmente essere illustrati:

- Metodologia proposta;
- Organizzazione del servizio;
- Gruppo di lavoro;
- Qualifiche professionali;
- Esperienza;
- Piano delle attività;
- Giornate/uomo;
- Metodologia VA/PT;
- Strumenti e metodologie di sicurezza;
- Modalità di reporting;
- Tempi di esecuzione.

Per il Lotto 2, nella relazione illustrativa, dovranno possibilmente essere illustrati:

- Accreditamento;
- Organizzazione dell'audit;
- Gruppo di auditor;
- Esperienza;
- Programma indicativo;
- Giornate di audit.

45. MANCATA AGGIUDICAZIONE

La Stazione Appaltante si riserva, nei limiti consentiti dalla normativa applicabile, il diritto di non procedere all'aggiudicazione.
La partecipazione alla procedura non comporta alcun diritto all'affidamento.
Non sorgeranno diritti o pretese in capo ai partecipanti fino all'adozione del provvedimento di aggiudicazione e alla sottoscrizione del relativo contratto.

46. ALLEGATI TECNICI

Costituiscono, ove disponibili, documenti di riferimento per l'esecuzione del servizio:

1. Certificato ISO/IEC 27001:2022 n. **71347/A/0001/UK/It**;
2. Documento di Analisi del Contesto del SGSI;
3. Eventuale ulteriore documentazione relativa allo scope.

47. CRONOPROGRAMMA INDICATIVO

Periodo	**Lotto 1 - Supporto, Analisi e VA/PT**
2026	Gap Analysis, aggiornamento SGSI, VA/PT, Risk Assessment, SoA, audit interno, remediation, preparazione audit: entro novembre 2026
2027	Mantenimento SGSI, aggiornamento documentazione, VA/PT, Risk Assessment, SoA, audit interno, azioni correttive: entro novembre 2027
2028	Preparazione rinnovo, aggiornamento SGSI, VA/PT, Risk Assessment, SoA, audit interno, supporto ricertificazione: entro agosto 2028

Periodo	**Lotto 2 – Certificazione**
2026	Audit di sorveglianza entro dicembre 2026
2027	Audit di sorveglianza entro dicembre 2027
2028	Audit di ricertificazione entro settembre 2028