PREGLED POSTUPKA #120751

1 PODACI O NARUČIOCU

Naziv naručioca	LUKA BAR AD
PIB	02002558
E-mail	kabinet@lukabar.me
Telefon	030/300-400
Internet adresa	www.lukabar.me
Fax	030/300-402
Adresa	Obala 13.jula 2
Grad	Bar
Poštanski broj	85000

2 OSNOVNI PODACI

Opis predmeta javne nabavke	Implementacija standarda ISO 27001
Status	U izradi
Vrsta predmeta	Usluge
Vrsta postupka	Jednostavna nabavka
Službenik za javne nabavke	Sonja Stanišljević
Kontakt	H.Čuturić (067/333-097)
Datum objave	27.08.2026. 14:00

Napomena	Sertifikacija nije predmet ove nabavke i sprovodi se posebno, po završetku projekta implementacije, kroz odvojen postupak javne nabavke.

3 FAZE U POSTUPKU

Nema faza u izabranom postupku

4 DODATNE INFORMACIJE

Predmet javne nabavke se nabavlja	kao cjelina
Posebni oblici javne nabavke	
Okvirni sporazum	Ne
Dinamički sistem nabavki	Ne
Elektronska aukcija	Ne
Elektronski katalog	Ne
Nabavka se sprovodi kao	
Zajednička nabavka	Ne
Centralizovana nabavka	Ne
Nabavka je	
Zelena	Ne
Društveno odgovorna	Ne

5 STAVKE PLANA

Godina	Opis	Vrijednost nabavke	Vrijednost PDV	Okvirni sporazum	Vrijednost OS	Vrijednost PDV OS	Vrsta postupka
2026	**LUKA BAR AD** **Usluga konsaltinga za uvođenje ISO standarda i sertifikacija** 79000000 - Poslovne usluge: pravne, marketing, konsalting, zapošljavanje, štampanje i bezbjednost	24.000,00 EUR	5.040,00 EUR	-	-	-	Jednostavna nabavka

6 USLOVI ZA UČEŠĆE U POSTUPKU I ZAHTJEVI U POGLEDU NAČINA IZVRŠAVANJA PREDMETA NABAVKE

Opis	Tip uslova / zahtjeva
Privredni subjekat je dužan da posjeduje minimum stručnih i kadrovskih kapaciteta koji su potrebni za izvršenje ugovora. Stručna i tehnička sposobnost dokazuje se dokazom o angažovanju radne snage (prijava za osiguranje zaposlenog, ugovor o radu, sporazum o preuzimanju zaposlenog, ugovor o korišćenju sposobnosti drugog subjekta ili drugi akt u skladu sa zakonom) i to: Lead Auditor - 1 konsultant, koji mora posjedovati važeći personalni sertifikat vodećeg (eksternog) auditora za ISO/IEC 27001 — ISO/IEC 27001 Lead Auditor, stručnjak za menadžment rizikom - 1 konsultant, koji mora posjedovati važeći personalni sertifikat iz oblasti menadžmenta rizikom u skladu sa ISO 31000 ili ekvivalentnu međunarodno priznatu kvalifikaciju s obzirom na to da je procjena i tretman rizika važan dio ISMS-a i eksperta za zaštitu ličnih podataka, koji posjeduje sertifikat CDPSE (Certified Data Privacy Solutions Engineer) i/ili osposobljen za ISO/IEC 27701 (sistem menadžmenta privatnošću informacija).	Stručna i tehnička sposobnost
Privredni subjekat je dužan da posjeduje minimum iskustva na kvalitetnom i uspješnom izvršavanju poslova iz oblasti predmeta nabavke. Stručna i tehnička sposobnost dokazuje se potvrdama, izdatim od strane korisnika, o izvršenim uslugama implementacije sistema menadžmenta bezbjednošću informacija u skladu sa standardom ISO/IEC 27001, tokom prethodnih godina, ali ne duže od pet godina, računajući i godinu u kojoj je započet postupak javne nabavke, koje sadrže opis pružene usluge, mjesto pružanja usluge, vrijednost pružene usluge, vrijeme realizacije ugovora uz konstataciju da je ugovor blagovremeno i kvalitetno izvršen. Privredni subjekat je u obavezi da u ponudi dostavi dokaze (potvrde) da je izvršio najmanje osam usluga implementacije standarda ISO 27001.	Stručna i tehnička sposobnost

Uz ponudu se dostavlja izjava ponuđača o ispunjenosti uslova utvrđenih zahtjevom o nepostojanju sukoba interesa, potpisana od strane ovlašćenog lica ponuđača, data na Obrascu 2, preuzimanjem na posebnom aplikativnom dijelu elektronskog sistema javnih nabavki, shodno članu 9 stav 10 i 11 Pravilnika o načinu sprovođenja jednostavnih nabavki („Službeni list Crne Gore“, br. 016/23 od 10.02.2023. godine, 020/23 od 22.02.2023. godine, 036/23 od 29.03.2023. godine, 114/23 od 19.12.2023. godine, 049/24 od 29.05.2024. godine, 114/24 od 29.11.2024) potpisana elektronskim potpisom.	Obrazac 2
Rok izvršenja ugovora je maksimalno 150 kalendarskih dana od dana potpisivanja ugovora (mora biti naveden isti broj dana kao u kriterijumu za izbor najpovoljnije ponude).	Rok izvršenja ugovora
Mjesto izvršenja ugovora je sjedište "Luka Bar" AD Bar, na adresi Obala 13. jula broj 2 i kancelarije izabranog ponuđača.	Mjesto izvršenja ugovora
Plaćanje će se izvršiti na način što će se u roku od 15 kalendarskih dana od dana obostrano potpisanog završnog izvještaja o pripremi za sertifikaciju izabranom ponuđaču uplatiti 70% ugovorene vrijednosti ugovora, dok će se ostalih 30% ugovorene vrijednosti ugovora uplatiti izabranom ponuđaču u roku od sedam kalendarskih dana od dana sertifikacije.	Rok plaćanja
Način plaćanja je virmanski, na žiro račun Izabranog ponuđača. Žiro račun:_____ Banka:_____ (Ponuđač je obavezan navesti broj žiro računa i banke).	Način plaćanja
Uslovi plaćanja su: obostrano potpisani završni izvještaj o pripremi za sertifikaciju, sertifikacija i ispravne fakture.	Uslovi plaćanja
□ Sertifikat ISO 9001 Ponuđači su dužni dostaviti važeći sertifikat ISO 9001 (sistem menadžmenta kvalitetom), izdat od akreditovanog sertifikacionog tijela; □ Sertifikat ISO/IEC 27001 Ponuđači su dužni dostaviti važeći sertifikat ISO/IEC 27001 (sistem menadžmenta bezbjednošću informacija), izdat od akreditovanog sertifikacionog tijela — kao dokaz da i sam primjenjuje standard koji uvodi; □ Sertifikat za sprovođenje obuka Ponuđači su dužni dostaviti važeći sertifikat kojim se potvrđuje njegov status sertifikovanog ili priznatog pružaoca obuka, izdat od međunarodno priznatog tijela za sertifikaciju osoblja i pružalaca obuka.	Dokaz odnosno sertifikat, koje izdaju akreditovana sertifikaciona tijela o ispunjavanju uslova kvaliteta predmeta nabavke
Izabrani ponuđač je dužan izvršiti osnovnu obuku najmanje četiri zaposlena kod Naručioca, i to za nivo internog auditora, sa međunarodno priznatim sertifikatom.	Stručno osposobljavanje

Naručilac je u obavezi da imenuje vođe projekta i projektnog tima (predstavnike organizacionih jedinica), obezbijedi pristup informacijama, dokumentaciji i prostorijama, kadrovsku i tehničku podršku tokom realizacije projekta, kao i da učestvuje u recenziji i primjeni dokumentacije i da imenuje zapolesne za obuku internog auditora.	Drugi uslovi
Izabrani ponuđač je u obavezi da minimum pet radnih dana, o svom trošku, provede na lokaciji Naručioca.	Drugi uslovi
Izabrani ponuđač je dužan da za vrijeme trajanja implementacije i prilikom sertifikacije bude online dostupan, kao i da Naručiocu pruži podršku u otklanjanju utvrđenih neusaglašenosti.	Drugi uslovi

7 KRITERIJUMI ZA IZBOR NAJPOVOLJNIJE PONUDE

Opis
Cijena
U okviru podkriterijuma kvalitet vrednovaće se rok izvršenja predmeta nabavke, na način što se najmanji ponuđeni rok izvršenja predmeta nabavke podijeli sa ponuđenim rokom izvršenja predmeta nabavke i dobijeni količnik pomnoži sa brojem bodova koji je određen za ovaj podkriterijum – 30 bodova po formuli: Broj bodova= C (Najmanji ponuđeni rok izvršenja predmeta nabavke) / C (Ponuđeni rok izvršenja predmeta nabavke) * 30. Minimalan rok izvršenja predmeta nabavke je 120 kalendarskih dana, dok je maksimalan rok izvršenja predmeta nabavke 150 kalendarskih od dana potpisivanja ugovora. Ponuđači su obavezni da rok izvršenja predmeta nabavke prikažu u kalendarskim danima (cijeli brojevi).

8 PREDMET NABAVKE

Procijenjena vrijednost nabavke: **7.000,00 EUR**

TEHNIČKA SPECIFIKACIJA PREDMETA NABAVKE

	Opis predmeta nabavke	Bitne karakteristike predmeta nabavke	Količina
		Opseg sistema Implementacija ISMS-a odnosi se na kompletnu organizaciju Naručioca — sve organizacione jedinice, sektore, poslovne procese i lokacije na kojima "Luka Bar" AD Bar obavlja svoju djelatnost. Konačan opseg sistema, uključujući granice i primjenjivost, definiše se u početnoj fazi projekta, u saradnji Naručioca i izabranog ponuđača, uz posebno uvažavanje specifičnosti lučke djelatnosti, kritične infrastrukture i informacionih sistema od značaja za kontinuitet poslovanja. Obim implementacije — dokumentacija i kontrole U okviru projekta izabrani ponuđač je dužan da uspostavi kompletan, dokumentovan i primjenjiv sistem menadžmenta bezbjednošću informacija (ISMS), koji obuhvata najmanje sljedeće: Dokumentacija sistema • politiku bezbjednosti informacija i ciljeve bezbjednosti informacija, usklađene sa strateškim ciljevima Naručioca; • potrebne politike, procedure i druge dokumentovane informacije u skladu sa zahtjevima standarda; • obrasce i dokaze o funkcionisanju sistema; • metodologiju ocjenjivanja rizika, registar rizika i plan postupanja sa rizikom;	

1	Pružanje konsultantskih usluga na uvođenju i implementaciji sistema menadžmenta bezbjednošću informacija (u daljem tekstu: ISMS) prema zahtjevima međunarodnog standarda	• Izjavu o primjenjivosti (Statement of Applicability — SoA). Zahtjevi standarda Izabrani ponuđač je dužan da kod Naručioca uspostavi sistem menadžmenta bezbjednošću informacija (ISMS) koji ispunjava sve obavezne zahtjeve standarda ISO/IEC 27001 sadržane u tačkama od 4 do 10: Tačka 4 — Kontekst organizacije: utvrđivanje internih i eksternih pitanja, zainteresovanih strana i njihovih zahtjeva, te određivanje predmeta i područja primjene (opsega) sistema. Tačka 5 — Liderstvo: liderstvo i posvećenost rukovodstva, politika bezbjednosti informacija, te uloge, odgovornosti i ovlašćenja. Tačka 6 — Planiranje: postupanje sa rizicima i prilikama, ocjenjivanje i postupanje sa rizikom po bezbjednost informacija i utvrđivanje ciljeva bezbjednosti informacija. Tačka 7 — Podrška: resursi, kompetentnost, svijest, komunikacija i dokumentovane informacije. Tačka 8 — Operativne aktivnosti: operativno planiranje i upravljanje, ocjenjivanje rizika po bezbjednost informacija i postupanje sa rizikom po bezbjednost informacija. Tačka 9 — Vrednovanje performansi: praćenje, mjerenje, analiza i vrednovanje, interna provjera i preispitivanje od strane rukovodstva. Tačka 10 — Poboljšavanje: postupanje sa neusaglašenostima, korektivne mjere i stalno poboljšavanje sistema. Kontrole bezbjednosti informacija Izabrani ponuđač je dužan da kod Naručioca primijeni sve kontrole iz Aneksa A standarda ISO/IEC 27001 koje su primjenjive i kao takve utvrđene Izjavom o primjenjivosti (SoA).	1,00 komplet

	ISO/IEC 27001:2022, koji je u Crnoj Gori usvojen od strane Instituta za standardizaciju Crne Gore (ISME), kao crnogorski standard pod oznakom MEST EN ISO/IEC 27001:2024.	Prema važećem izdanju standarda, Aneks A obuhvata ukupno 93 kontrole, razvrstane u četiri grupe: A.5 Organizacione kontrole — obuhvataju kontrole koje se odnose na organizaciju bezbjednosti informacija, uloge i odgovornosti, informacije i drugu povezanu imovinu, kontrolu pristupa, odnose sa isporučiocima, menadžment incidentima narušavanja bezbjednosti informacija, kontinuitet poslovanja i usaglašenost sa relevantnim zahtjevima. A.6 Kontrole ljudi — obuhvataju kontrole koje se odnose na provjeru i uslove zapošljavanja, svijest, obrazovanje i obuku o bezbjednosti informacija, disciplinski postupak, odgovornosti poslije promjene ili prestanka zaposlenja, povjerljivost, rad na daljinu i izvještavanje o događajima u vezi sa bezbjednošću informacija. A.7 Fizičke kontrole — obuhvataju kontrole fizičke bezbjednosti prostorija, opreme i druge povezane imovine, fizičkog pristupa, zaštite od fizičkih prijetnji i prijetnji iz okruženja, medijuma za skladištenje, kablovskih instalacija i održavanja opreme. A.8 Tehnološke kontrole — obuhvataju kontrole koje se odnose na pristup informacijama i informacionim sistemima, autentifikaciju, zaštitu od zlonamjernog softvera, tehničke ranjivosti, konfiguraciju, rezervne kopije, logove i praćenje, bezbjednost mreža, kriptografiju, bezbjedan razvoj i zaštitu informacionih sistema. Ponuđač je dužan da obezbijedi odgovarajuće dokumentovane informacije i dokaze o primjeni i funkcionisanju svih primjenjivih kontrola u praksi. Faze realizacije projekta Realizacija projekta sprovodi se kroz pet međusobno	

		povezanih faza: I. Analiza postojećeg stanja Analiza postojećeg stanja u odnosu na zahtjeve standarda: pregled dokumentacije i akata, identifikacija procesa i informacionih sredstava, intervjui sa timom koji će raditi na projektu i ključnim osobljem, utvrđivanje opsega (scope) i granica sistema. Isporuka: Izvještaj o postojećem stanju. II. Izrada dokumentacije i uspostavljanje ocjenjivanja rizika Uspostavljanje metodologije ocjenjivanja rizika, registra rizika i Izjave o primjenjivosti (SoA), izrada kompletne dokumentacije ISMS-a (politike, procedure, uputstva, obrasci i dr.), definisanje konteksta organizacije, uloga, odgovornosti i ciljeva bezbjednosti informacija. III. Primjena kontrola prema Aneksu A Primjena organizacionih kontrola, kontrola ljudi, fizičkih i tehnoloških kontrola u obimu utvrđenom Izjavom o primjenjivosti (SoA), uz obezbjeđivanje dokaza o njihovoj primjeni i funkcionisanju u praksi. IV. Obuka zaposlenih V. Interna provjera i priprema za sertifikaciju	