ANEKS A – Tender 1

Specifikime Teknike – Asistencë për Dokumentacionin ISMS sipas ISO 27001:2022 për SiCRED

1. Objekti i kontratës

Asistencë në rishikimin dhe zhvillimin e dokumentacionit të Sistemit të Menaxhimit të Sigurisë së Informacionit (ISMS) në përputhje me ISO 27001 për SiCRED, duke përfshirë rishikimin e kornizës dhe politikave të qeverisjes së IT.

2. Qëllimi i kontratës:

Ofrimi i ekspertizës profesionale për hartimin dhe standardizimin e dokumentacionit të Sistemit të Menaxhimit të Sigurisë së Informacionit (ISMS), sipas kërkesave të ISO 27001, për të siguruar përputhshmëri, kontroll të rreziqeve dhe rritje të nivelit të sigurisë së informacionit në SiCRED.

Nëpërmjet këtij projekti SiCRED synon te sigurojë integrimin e komponentëve ekzistues kritik te infrastrukturës se tij për forcimin e pozicionit të përgjithshëm të sigurisë dhe arritjen e përputhshmërisë me ligjet ne fuqi.

3. Arsyetimi dhe konteksti rregullator

Përzgjedhja e standardit ISO 27001:2022 si udhërrëfyesi kryesor i zbatimit është strategjikisht e përafruar me kërkesat e përputhshmërisë së SiCRED dhe objektivat e maturimit organizativ, meqenëse ky standard ofron një kornizë të qartë dhe të plotë për:

- "masat teknike dhe organizative të duhura" të referuara në Ligjin 124/2024 (Neni 22),
- "kontrollet teknike të sigurisë" të kërkuara nga Ligji 25/2024 (Neni 20), si dhe
- "përgjegjësinë e organit drejtues" të kërkuar nga DORA (Neni 11)
- Ofruesi duhet të dorëzojë një 'control-to-regulation traceability matrix' që hartëzon secilin kontroll të ISMS kundrejt:
  - Ligjit 124/2024,
  - Ligjit 25/2024,
  - Kërkesave të qeverisjes sipas DORA,

  duke treguar mbështetjen që secili kontroll i ISMS i jep përputhshmërisë rregullatore.

4. Përshkrimi i punës (Scope of Work)

- Rishikim i gjendjes aktuale të dokumentacionit ISMS dhe kornizës së qeverisjes së IT (gap analysis).
- Hartim/rihartim i dokumenteve kryesore të ISMS sipas ISO 27001:2022.
- Konsolidim i politikave dhe procedurave ekzistuese; unifikim terminologjik dhe versionim.
- Ndërtim i regjistrave të detyrueshëm (risk, asete, trajnime, incidente, audit, rishikim menaxhmenti).
- Përgatitje për audit të brendshëm dhe rishikim menaxhmenti (templates, udhëzues, agenda).
- Përcaktimin e:

- Qëllimit dhe shtrirjes së ISMS
- Palët e interesuara dhe kërkesat e tyre
- Proceset e ISMS-it dhe ndërveprimi i tyre

5. Deliverables

Seti i dorëzuesve do të strukturohet në tre kategori:

- Dokumentacioni Bazë (Foundation)
  - A.5 Information Security Policies
  - A.5 9 Asset Management & Inventory
  - A.5 36 Compliance with policies, rules and standards for information security
  - ISO 31000 Risk Management (RMS)
  - A.5.30 ICT Readiness for Business Continuity ose ISO 22301 Business Continuity
- Kontrollet thelbësore
  - A. 5.15 Access Control
  - A. 8.24 Use of Cryptography
  - A. 7.1, A.7. 2, A.7.3, A.7.4, A.7.5 Controls Related to Physical Security
  - A. 5.26 Response to information security incidents
- Kontrollet e Avancuara
  - A. 8.25, A.5.26, A.5.27, A.5.28, A.5.29 Controls Related to System Development
  - A. 5.24 Information security incident management planning and preparation
  - A. 5.19, A.5.20, A.5.21, A.5.22 Controls Related to Supplier Relationships/Third Parties
  - A. 5.7 Threat intelligence

6. Kriteret e Kualifikimit për Ofruesin e Shërbimit

6.1. Kriteret e Kapacitetit Teknik dhe Profesional

Ofruesi duhet të demonstrojë se ka aftësi të provuara në ofrimin e shërbimeve të sigurisë së informacionit, përfshirë:

- Eksperiencë e dokumentuar në projekte implementimi ose rishikimi të ISO/IEC 27001 në 3–5 vitet e fundit.
- Minimumi 2 projekte të ngjashme në organizata të sektorit financiar, sigurimeve, bankave, telekomit ose institucioneve kritike.
- Staff teknik i certifikuar në të paktën një nga këto:
  - ISO 27001 Lead Implementer
  - ISO 27001 Lead Auditor
  - CISA / CISM / CISSP (opsionale por e vlerësuar)
- Eksperiencë praktike në:
  - Hartim dokumentesh ISMS (politika, procedura, regjistra)
  - Risk management sipas ISO 31000 / ISO 27005
  - Incident management (Incident Responder)
  - Business Continuity (ISO 22301) — opsionale por e preferuar
  - Threat Intelligence Certified (opsionale por e vlerësuar)

- Kapacitet për të kryer gap analysis, risk assessment, SOA, procesverbal rishikimi, dhe audit të brendshëm.

6.2. Kriteret e Kapacitetit Organizativ

- Ekipi që ofron shërbimin duhet të ketë të paktën 2 ekspertë të profilit të lartë të sigurisë së informacionit.
- Ofruesi duhet të paraqesë një strukturë organizative të ekipit të projektit dhe rolet përkatëse.
- Duhet të sigurojë kontinuitet të stafit gjatë gjithë projektit (ndryshimet duhet të justifikohen).
- Ofruesi duhet te paraqesë dëshmi te qarta, dhe te dokumentuara qe vërtetojnë kualifikimet, përvojën dhe disponueshmerine e stafit te afte, te cilat janë te domosdoshme për realizimin e suksesshëm te projektit.

6.3. Kriteret e Kapacitetit Financiar

- Xhiroja vjetore e operatorit ekonomik në vitet e fundit të jetë jo më pak se 2–3 herë vlera e kontratës (standard në tendera publikë).
- Mosprania e detyrimeve të pashlyera tatimore ose sociale

6.4. Dokumente të detyrueshme që duhet të paraqiten

- CV të stafit kryesor.
- Kopje të certifikatave profesionale.
- Portofol projektesh të ngjashme (me përshkrim pune dhe kontakt reference).
- Deklaratë për mos-konflikt interesi.
- Deklaratë për disponueshmëri dhe angazhim në projekt.

6.5. Kriteret për Metodologjinë e Punës (evaluation criteria)

Ofruesi duhet të paraqesë:

- Qasjen metodologjike të implementimit / rishikimit të ISMS.
- Plan pune me faza, afate dhe deliverables.
- Qartësi në mënyrën e kryerjes së risk assessment, kontrollit të dokumentacionit, zhvillimit të politikave, dhe përgatitjes për audit.
- Propozim për knowledge transfer dhe trajnime për stafin e SiCRED.

6.6. Kritere të Cilësisë së Ofruesit

- Mekanizma të brendshëm të kontrollit të cilësisë.
- Standardet e brendshme që ndjek kompania (p.sh., ISO 9001 — opsionale).
- Disponueshmëri për asistencë gjatë auditimit të brendshëm ose të jashtëm.

7. Menaxhimi i projektit dhe afatet

Ofruesi do të propozojë planin e punës me faza dhe afate, për shembull:

- Faza 1 – Vlerësimi fillestar & Gap Analysis (2–3 javë).
- Faza 2 – Hartimi dhe standardizimi i dokumenteve (4–6 javë).
- Faza 3 – Zbatim pilot, trajnime dhe evidenca (2–3 javë).
- Faza 4 –Rishikim menaxhmentit (1–2 javë).

8. Bazë ligjore dhe standarde reference

- ISO/IEC 27001:2022 – kërkesat për ISMS.
- Ligji 124/2024 (Neni 22).
- Ligji 25/2024 (Neni 20).
- DORA (Neni 11)
- ISO 31000, ISO 22301.