NIS2 GRC Consultant

Profil

1. Role Context

We are looking for an experienced individual GRC consultant to support NIS2 compliance programme across Belgian and Italian entities (Essential and Important, manufacturing sector included). The consultant will run assessments, apply an agreed methodology, and produce the deliverables below.

2. Required Experience

- Has personally led or been a core assessor on NIS2 (or equivalent NIS/critical-infrastructure) assessments for a minimum of 5 Important Entities and 2 Essential Entities in Belgium, including at least 2 in manufacturing.
- Has personally led or been a core assessor on NIS2 (or equivalent) assessments for a minimum of 5 Important Entities and 2 Essential Entities in Italy, including at least 2 in manufacturing.
- Can provide at least 3 checkable references (client contacts or engagement managers) and describe 2–3 representative case studies (anonymised where confidentiality requires it).

3. Methodology

Candidate must be able to demonstrate, in their own words and with material where possible:

- Their personal NIS2 assessment methodology, and whether it follows a documented framework they can walk through.
- Working knowledge of NIST CSF as the control framework (required for both Belgium and Italy).
- Their evidence collection process (interviews, document review, technical evidence, sampling approach).
- Maturity model experience: CyFun for Belgium; CMMI preferred for Italy (no fixed national model there).
- How they structure reporting back to client stakeholders and management.

4. Deliverables the Candidate Must Be Able to Produce

- Gap assessment report
- Compliance status mapped per NIS2 article and applicable national legislation (Belgium and Italy)

- Risk register
- Executive presentation / summary for management
- Prioritised remediation roadmap
- Audit evidence repository
- Residual risk assessment

5. Competence & Certification

- Evidence of NIS2-specific training (certificates, course records).
- Demonstrable understanding of local NIS2 transposition in Belgium and Italy.
- CV detailing relevant engagements and role on each.
- Experience supporting regulatory inspections in the manufacturing sector.
- Ability to translate legal/regulatory requirements into practical, implementable controls.
- At least one relevant certification: ISO 27001 Lead Auditor, CISSP, or CISA.
- Total years of relevant GRC/audit experience (state explicitly).

6. Work Sample

Candidate to provide 1–2 anonymised sample reports for evaluation on:

- Clarity
- Executive-readiness
- Actionability
- Risk-based prioritisation
- Traceability back to specific NIS2 requirements

Others

Engagement Logistics

- Locations: Bari, Italy and Zaventem, Belgium (both legal entities in scope).
- Work pattern: audit preparation remote; the audit itself is expected onsite at each entity. Candidate/supplier to confirm their own remote/onsite split and specify which phases are onsite.

- Target start: early February 2027.
- Target deliverable: final audit report by mid-March 2027: candidate to propose a mission duration and day count that fits this deadline, working backward from mid-March.
- Suggested working pattern: 5 days/week if that is the most effective set-up for an external audit of this scope; open to alternative proposals if justified.