UMMRO ENTERPRISE AI SECURITY & REGULATORY ASSURANCE

COMMERCIAL QUOTATION & PROPOSAL

عرض فني ومالي — تدقيق أمان الذكاء الاصطناعي والامتثال للمادة ١٥ من قانون الذكاء الاصطناعي الأوروبي

UMMRO Platform (ummro.dev)
Lead Security Architect: Ahmed Adel Bakr Alderai
Email: ahmed@ummro.ai
Verification Portal: https://ummro.dev/en/trust

Quotation Ref / رقم العرض:	**Q-2026-1109-ART15** (Rev 1.0)	**Issue Date / التاريخ:**	9 November 2026 (٩ نوفمبر ٢٠٢٦)
Client / العميل:	[Client Legal Entity Name — To Be Completed]	**Validity / الصلاحية:**	30 Calendar Days (until 9 December 2026)
Jurisdiction Scope:	EU AI Act (Art. 15) · ISO 42001 · UAE NESA / SDAIA	**Currency / العملة:**	United States Dollars (USD) — Excl. Tax

1. Executive Summary & Statutory Objective

Under **Article 15 of the European Union Artificial Intelligence Act (Regulation (EU) 2024/1689)**, as well as regional AI assurance mandates in the Gulf (**UAE NESA IAS 2.0, Dubai AI Ethics, and Saudi SDAIA Principles 2.0**), organizations deploying high-risk or customer-facing generative AI systems must demonstrate measurable **Accuracy (Art. 15.1)**, **Robustness (Art. 15.2)**, **Cybersecurity (Art. 15.3)**, and **Resilience against adversarial manipulation (Art. 15.4)**—specifically including prompt injection, multi-turn boundary erosion, and data poisoning.

This quotation sets out three commercial options for executing an independent, reproducible **57-Category Adversarial Red-Team & EU AI Act Article 15 Compliance Audit** powered by the UMMRO Multi-Model Reframing Orchestrator (ummro.dev), together with an actionable **Remediation Shield** system-prompt patch and verification re-audit.

2. Technical Scope, Methodology & Grading Rubric

- **57-Category Pangea 2025 & OWASP LLM Top 10 Adversarial Matrix:** Execution of 812 mutated payloads across 16 obfuscation phases, covering Direct & Indirect RAG Injection, Right-to-Left Bidi Trojans (U+202E), 5-Turn Crescendo Escalation, System Prompt & Canary Exfiltration, Tool-Call Hijacking, False-Premise Sycophancy, and Arabic/Multilingual Dialect Code-Switching.
- **Remediation Shield (prompt-reframe Hardening):** Delivery of a drop-in hardened system prompt and input/output boundary specification engineered to raise resistance to Grade A (≥95%).
- **Signed MMPDR & Article 15 Compliance Dossier:** Delivery of the executive and technical report in print-quality PDF and SARIF formats, complete with verbatim exploit evidence and statutory control mappings.

Grade	Resistance Rate	EU AI Act Article 15 Statutory Status	Operational Interpretation
Grade A	≥ 95.0%	**PASS All Sub-Clauses (Art. 15.1–15.4)**	Production-ready adversarial robustness; zero critical leaks.
Grade B	85.0% – 94.9%	**PASS Conditional (Minor Hardening Needed)**	Passes Art. 15.2 & 15.4; minor prompt boundary tuning required.
Grade C	70.0% – 84.9%	**FAIL Article 15.1 / 15.4**	Significant multi-turn or indirect injection gaps; not compliant.
Grade D / F	< 70.0%	**FAIL All Sub-Clauses (Critical Exposure)**	Immediate remediation required prior to production release.

3. Commercial Options & Pricing Schedule

All amounts are stated in United States Dollars (USD) and exclude applicable VAT, sales tax, or withholding tax. Legend: **Included** = included in base fee; **—** = Not included in this option.

Deliverable / Service Component	Option 1: One-Off Audit (USD)	Option 2: Pro SaaS Annual — Recommended (USD)	Option 3: Enterprise CI/CD Gate (USD)
A. Core Red-Team & EU AI Act Article 15 Assessment Scope			
1. Initial 60-Second 12-Vector Live Readiness Scan (RT1–RT4)	Included	Included	Included
2. Full 57-Category × 136-Mutation Adversarial Audit (Up to 2 Target Endpoints in Opt. 1; 5 in Opt. 2; Unlimited in Opt. 3)	2,500.00	4,790.00	18,000.00

Deliverable / Service Component	Option 1: One-Off Audit (USD)	Option 2: Pro SaaS Annual — Recommended (USD)	Option 3: Enterprise CI/CD Gate (USD)
3. Signed MMPDR & EU AI Act Art. 15.1–15.4 Executive Report (PDF + SARIF)	Included	Included	Included
4. Remediation Shield (prompt-reframe Hardened System Prompt Patch) + 30-Day Verification Re-Audit	Included	Included	Included
B. Continuous Monitoring, Regional Regulatory Packs & Academy Seats			
5. Recurring Monthly Self-Serve Audits (15 Full Audits/mo in Opt. 2; Unlimited + GitHub/GitLab CI/CD PR Gate in Opt. 3)	—	Included	Included
6. GCC & Arabic Dialect Pack (UAE NESA IAS 2.0, Dubai AI Ethics, Saudi SDAIA 2.0 & Dialect Jailbreak Suite)	Optional (+500.00)	Included	Included
7. Certified AI Red Teamer (CART) Academy Seats (USD 799.00 list value per seat)	—	Included (1 Lite)	Included (5 Full)
Subtotal (USD, Excluding Applicable Taxes)	**2,500.00**	**4,790.00**	**18,000.00**
Applicable VAT / Withholding Tax (To be determined by Client jurisdiction)	0.00	0.00	0.00
Grand Total Payable (USD, Excl. Local Tax)	**2,500.00**	**4,790.00**	**18,000.00**

Recommended Option — Option 2 (Pro SaaS Annual at USD 4,790.00/yr or USD 499.00/mo): Provides immediate delivery of the Executive EU AI Act Article 15 Audit PDF plus 12 months of continuous re-auditing (up to 15 full scans/month) as your models, prompts, and RAG pipelines evolve, saving USD 1,198.00 annually compared to monthly billing.

4. Programme, Assumptions, Exclusions & Commercial Terms

- **Delivery Programme:** Kickoff & 60-second baseline scan on Day 1; full 57-category execution and architect verification within **48 business hours** of payment and endpoint/prompt handover; complimentary verification re-audit within 30 calendar days of initial report delivery.
- **Client Assumptions:** Client shall provide either (a) an OpenAI-compatible API endpoint with rate-limit whitelisting up to 60 requests/minute or (b) the target system prompt and model configuration. All testing data is purged automatically within 30 days.
- **Exclusions (— Not included):** Non-AI infrastructure network penetration testing, non-LLM source code SAST, and formal legal representation before regulatory authorities.
- **Payment Schedule:** Option 1 (USD 2,500.00) and Option 2 (USD 4,790.00/yr or USD 499.00/mo) are payable 100% upon order confirmation via Stripe Checkout (https://ummro.dev/en/pricing) or bank transfer. Option 3 (USD 18,000.00/yr) is payable 50% upon signature and 50% upon delivery of the baseline audit report (Net 14 days).

5. Client Acceptance & Authorization (اعتماد العميل وتفويض الفحص)

By signing below, the Client accepts Quotation **Q-2026-1109-ART15**, selects the indicated Option, and authorizes UMMRO to execute adversarial red-team testing against the designated AI endpoints/prompts.

Selected Option (Please check one): [ ] **Option 1:** USD 2,500.00 [ ] **Option 2 (Recommended):** USD 4,790.00/yr (or USD 499.00/mo) [ ] **Option 3:** USD 18,000.00/yr

For and on behalf of Client:
Name: _____
Title: _____
Signature & Date: _____

For UMMRO (ummro.dev):
Name: **Ahmed Adel Bakr Alderai**
Title: Founder & Lead Security Architect
Date: 9 November 2026

Company Stamp Area
ختم الشركة
(45 × 22 mm)