Value Proposition Letter

Peter Kirkov

Executive Summary

I am a European cybersecurity executive who operates at the regulator–practitioner intersection: a former National Cybersecurity Coordinator who has built Security Operations Centers at a national scale, led IT audits of major European banks, and now advises organizations through vCISO engagements on the operationalization of DORA, NIS2, PCI-DSS, ISO 27001, and ISO 42001. My career has been defined by taking single-firm accountability for cyber and information security posture in environments where the regulatory bar is high, the threat surface is meaningful, and the Board expects the CISO to be a peer of the CRO and CIO.

What I bring is not a single competency but the integration of four operating capabilities that most organizations hire separately: detection-and-response engineering, ISMS and audit discipline, executive and regulator communication, and crisis leadership under adversarial pressure. Those four are exactly the dimensions on which a regulator-grade cyber resilience program is judged under DORA.

Organisational Impact

In my career, I have built and run multiple things that a Tier-1 regulated enterprise CISO is now expected to deliver concurrently:

- **Operational 24/7 SOC** - National SOC for government networks (€5M programme); Strategic Sites SOC for critical national infrastructure (€6M programme); supported development of private-sector MSSP SOC at Telelink; NSOC and Strategic Sites SOC delivered under EU Internal Security Fund, and while technical details are classified, the projects and the results showing 100% goal achieved on time and within budget. I've also redesigned and implemented a new architecture for the National CSIRT to enable a countrywide federated infrastructure, ready for the integration of new sectoral CSIRT teams after the adoption of NIS2.
- **Regulator-defensible ISMS** - ISO 27001 certification on first attempt with minimal advisories — in both public and private-sector contexts, using my experience of actually working on NIS2 and other regulatory texts, including transposing regulations to national legislation.
- **Board-level cyber risk function** - Translating requisition requirements, threat intelligence, and incident data into the language the CRO, COO, and Management Board can understand to support decision making. I've briefed Cabinet-level cybersecurity boards in Bulgaria; board-level risk committees at European banks (Deloitte ERS).
- **Cross-boundary incident response** - National-level coordination across law enforcement, military, intelligence, regulators, and private sector — against APT-grade adversaries. I've worked with multiple other EU and UK cybersecurity authorities and institutions on cooperation and strategy. I've handled a zero-day nation-state DDoS campaign affecting large organizations and critical economic sectors in Bulgaria; coordinated with the CyCLONe/EU CSIRT Network; and was instrumental in establishing cooperation between Cloudflare and the EU CSIRT Network.

- **Team building across operational extremes -** Standing up, turning around, and leveling up teams where little is shared beyond the need for capable people. In the Big I led advisory and engagement teams of 10–18 on a billable, reputation-driven model; in government, I built 30+ team from a standing start and set the inspection, legal support, shift, escalation, and retention disciplines that keep a 24/7 function alive. Harder still are teams I don't control: coordinating 10+ organizations and partner authorities across the National CSIRT Network or National Cybersecurity Council meant assembling trust into a functioning response with no chain of command to fall back on.

My advantage is that most candidates offer one or two of these. I have built and run all four simultaneously, under the same regulatory frameworks (DORA, NIS2, ISO 27001) that now govern the institutions I am engaging with.

My differentiators

I Have Sat on the Regulator's Side of the Table

As Bulgaria's National Cybersecurity Coordinator, I contributed to the development and later transposition of NIS2 into national law, and I represented Bulgaria as an alternative member of the governing boards of both ENISA (EU Cybersecurity agency) and the European Cybersecurity Competence Center (ECCC, an agency that is responsible for funding all cyber projects in the EU). For any institution under multi-supervisor oversight, the value of a CISO who can interpret supervisory expectations from the inside and has a personal network within those institutions is significant.

I Have Both Audited Banks and Defended Them

At Deloitte, I led the IT audits of most major Bulgarian banks and served as the network expert for IT audit training across six CEE offices (Bulgaria, Romania, Albania, Slovakia, Slovenia, Belgium). I know the recurring findings that IT audit and the regulator raise in banking-sector cyber reviews, and I know how to close them operationally, not just on paper. This means my control designs survive first-line and second-line scrutiny because they were built with the auditor's lens from the start. I'm recognized on the market and keep supporting establishing and building banking functions – most recently in 2026, I've delivered specialized 2-week training for IT audit for DSK Bank Bulgaria (part of OTP)

I have an ISO 42001 Lead Auditor cert and Building AI-Security Tooling.

I hold both ISO 27001 Lead Auditor and ISO 42001 Lead Auditor certifications, and I co-founded Stihia, an AI-security startup focused on prompt-injection and rogue-agent detection. As regulated enterprises scale AI in risk functions, client-facing channels, and back-office operations, this combination means I can speak to model risk, EU AI Act compliance, and the security of AI agents from operational experience.

Specific Outcomes I Have Delivered

- **Operational SOC builds** - 3 (National SOC, Strategic Sites SOC, Telelink SOC), €11M+ EU-funded programs; Led Bulgarian part of Transnational SOC project pilot (Athena) under ECCC; Rebuilt National CSIRT architecture to enable sharing of operational cyber information.
- **Certifications**: 10+ first-attempt ISO 27001 certifications with minimal advisories, PCI-DSS certifications for the fintech sector, the public sector, financial services, and critical infrastructure compliance projects.
- **EU regulatory contribution -** NIS2 & CRA transposition; ENISA & ECCC governing board representation. Direct input to the frameworks now governing the EU, and especially the financial sector, on cyber resilience
- **Audit programs including financial sector - IT audits of most major Bulgarian banks; audit training deployed across 6 CEE Deloitte offices, Develop an audit program** for track and trace EU level audits in highly regulated sectors (pharma/tobacco).
- **Crisis leadership -** National-level incident coordination, including APT campaigns, election-infrastructure attacks. Coordinated across law enforcement, military, intelligence, private sector, and public communication.
- **Team building** – ranging from 10 - 18 person consulting teams; 30+ government organization teams; cross-country training delivery in Deloitte and multiple trans-organizational teams focused on efficiently achieving goals.
- **AI governance** ISO 42001 Lead Auditor; co-founder Stihia (prompt-injection/rogue-agent detection in agentic AI environment), I'm one of the few CISOs globally with dual 27001/42001 LA + operational AI security building experience.

Capabilities I Bring to the Organization

Regulatory Translation & Program Design

- **Build once, audit forever** - I design cyber programs so that audit is a derivative output, not a parallel project. DORA ICT risk framework, PCI-DSS, NIS2, and the AI management system share the same governance spine.
- **Regulation-to-control translation** - I understand the translation from an article in regulations and standards down to a specific control, a specific owner, and a specific evidence artifact.
- **Regulator as stakeholder, not adversary** - I treat supervisory bodies as a stakeholder group I have worked with, not as an external body. This enables wider cooperation and often unlocks new approaches.

Detection & Response Engineering

- **SOC architecture** from the ground up — SIEM/SOAR selection, log-source onboarding, detection-rule lifecycle, tiered triage, threat-hunting program, teams integration.
- **Tool rationalisation & automation** — Consolidation of fragmented stacks; SOAR-driven Tier-1 triage with human-in-the-loop controls; measurable MTTD/MTTR improvement.
- **Talent strategy** — Structured rotation, in-house development tracks, selective external hiring where needed, cloud security.

Third-Party & Supply-Chain Resilience

- **Top-down criticality inventory** — Ranked ICT third-party providers by criticality and substitutability, deep understanding of capabilities and competencies, and matching them to organizational needs.
- **Exit strategies & concentration testing** — Re-architected exit plans and substitutability tests for critical providers and partners, multi-level supply chain risk mapping.
- **Contractual & operational controls** — Operationalized register of provisions required by DORA RTS / equivalent regimes; embedded into existing TPRM tooling.

AI Security & Governance

- **AI Risk & Security Council design** — CISO-chaired, with CRO, CDO, Model Risk, Legal as standing members.
- **ISO 42001-aligned EU AI act compliant AIMS** — Classification of all AI use cases under EU AI Act risk taxonomy; model-security and prompt-injection detection deployment.
- **Deepfake & identity fraud controls** — Customer-facing and internal controls for AI-driven interactions.

Crisis Leadership & Board Communication

- **Crisis-response plans** tested at the national level - Integrated regulator-facing communications with internal crisis-management structure.
- **Senior-executive personal cyber protection** — Baseline and program for high-value Board and C-suite communications security.
- **Board reporting** - KPI/KRI dashboards and reports that can translate technical posture into risk-appetite language.

Long-Horizon Agility

- **PQC migration roadmaps** - Aligned to G7 Cyber Expert Group / BSI / NIST guidance; sequenced by data-sensitivity lifetime, not vendor roadmaps.
- **EU sovereignty initiative** - Reduced exposure to non-EU providers and jurisdictions to decrease geopolitical risks, mapped against EU Cloud Sovereignty Certification, Gaia-X, and data-localization requirements without sacrificing operational capability.