

NIS2 Consulting & Implementation

Compliance is not optional. Management liability is now personal.

The NIS2 Directive, transposed as OUG 155/2024, places direct personal liability on management for cybersecurity governance failures. Essential and important entities across energy, transport, healthcare, and finance must demonstrate full, auditable compliance or face significant financial penalties and operational restrictions. We make compliance real and sustainable — not just documented on paper and forgotten.

€10M**MAX FINE**

or 2% of global annual turnover for essential entities under NIS2

24h**REPORTING**

mandatory window to notify DNSC of significant incidents post-detection

87%**NOT READY**

of Romanian NIS2-subject companies lacked full compliance as of 2025

100%**MGMT LIAB.**

personal management liability for all cybersecurity governance failures

Our NIS2 Services

1

Gap Analysis & Risk Assessment

We audit your current posture against every NIS2 requirement and produce a prioritized gap report — showing exactly where you stand and precisely what must change.

3

Technical Controls (MFA/PAM/PKI)

Multi-Factor Authentication, Privileged Access Management, and PKI — implemented correctly and configured specifically for your environment, not a generic template.

5

DNSC Incident Reporting

We establish your detection, classification, and reporting workflows — ensuring mandatory notifications reach DNSC within the required legal timeframes consistently.

2

Security Policy Design

Organizational Security Plan (PSO), governance framework, access control policies, and technical standards aligned to CSF 2.0 and CRISC requirements throughout.

4

Business Continuity & DR

BCP and Disaster Recovery procedures designed and tested to meet NIS2 resilience requirements, validated against the mandated recovery timeframes for your specific sector.

6

Ongoing Compliance Management

Regular risk reviews, vulnerability cycles, training records, and audit-ready documentation — NIS2 is a continuous obligation, not a one-time project to complete once.

Why NIS2 Cannot Be Deferred

Personal Liability

NIS2 places explicit legal accountability on board members and senior management individually. Ignorance is not a valid defense under Romanian OUG 155/2024.

Penalties Are Severe

Essential entities face fines up to €10M or 2% of global turnover. Important entities face €7M or 1.4% turnover, with possible operational restrictions imposed.

Supply Chain Obligations

NIS2 requires you to manage the cybersecurity risk of your suppliers and service providers — extending your compliance obligation well beyond your own organizational perimeter.

What You Gain

A Full Legal Compliance

Every NIS2 requirement translated into concrete, auditable action — ready for regulatory inspection, partner due diligence reviews, and management board reporting.

B Protected Leadership

Documented governance structures and tested procedures demonstrate that management fulfilled its NIS2 obligations — shielding individuals from direct personal liability.

C Sustainable Posture

We stay with you through your first reporting cycle and beyond — because compliance achieved is only valuable when it is continuously maintained and adapted.

"

We went from zero NIS2 documentation to a full, auditable compliance posture in 11 weeks. Their team understood both the legal text and the technical reality of our infrastructure simultaneously.
— IT Manager, energy sector operator — NIS2 Implementation client

Do not wait for a regulatory inspection. Schedule a free NIS2 readiness assessment. secureintel.ro