VOICU ASOCIAȚII
Attorneys at Law

Business Catalysts

Legal Alert



NIS 2 after September 2026: "Practical Manual" for Compliance

Synopsis

The implementation in Romania of the new European directive on cybersecurity (NIS2) is entering, as of September 2026 and with Order No. 1/2026, a practical stage. For companies that have received the DNSC decision on their registration in the relevant register as essential or important entities, the compliance framework is finally becoming operational: deadlines start to run, and obligations must be addressed in a structured, documented manner, with careful prioritisation of risks. For companies still awaiting the decision, the new framework provides concrete benchmarks for anticipating and preparing their next steps.

FIRST STEP: assessing the risk level

The first step to be taken is submitting the risk level assessment to DNSC within 60 days from the communication of the decision.

The assessment shall be carried out pursuant to DNSC Order No. 2/2025, through **ENIRE@RO**, which calculates the risk score and the assurance level: Basic, Important or Essential.

Important: entities should not proceed on the assumption that classification as an "important entity" automatically entails the "Important" assurance level. The applicable level must be determined separately, based on the assessment carried out through ENIRE@RO.

The NIS2@RO platform is not yet available. What happens in the meantime?

Until the NIS2@RO Platform is launched, the assessment is carried out through ENIRE@RO, and the signed report, together with the supporting documents, is submitted to DNSC in accordance with the instructions communicated by the authority.

After the platform is launched, entities will have to create an account, enter the notification data and upload the report and supporting documents within a maximum of **20 days**.

SECOND STEP: self-assessment of maturity

Within 60 days from submitting the risk assessment, entities must carry out a self-assessment of the maturity of the cybersecurity measures applied. From a practical perspective, this exercise should be prepared in advance, as it involves both reviewing

the existing documentation and assessing the actual implementation of the relevant controls.

Provided for since Government Emergency Ordinance No. 155/2024, the obligation to conduct a **self-assessment of maturity** takes practical shape through the adjustment, under **DNSC Order No. 1/2026**, of the concrete measures and assessment methodology.

The Order is accompanied by two annexes:

- **Annex No. 1** – cybersecurity risk management measures;
- **Annex No. 2** – the methodology for the self-assessment of the maturity of these measures.

From general principles to concrete controls

Annex No. 1 includes **218 controls**, organised into **six functions**: Governance, Identification, Protection, Detection, Response and Recovery.

The controls are cybersecurity requirements and may include processes, policies, practices, devices or other risk management measures.

For each control, the annex includes a requirement and an indicative implementation guide; however, application should not be treated mechanically, but assessed specifically by reference to each entity's business profile, infrastructure, risk exposure and assurance level.

The controls apply differently depending on the assurance level, and their number and complexity increase from Basic to Essential.

How maturity is assessed

Annex No. 2 provides for scoring from 1 to 5 the maturity of the documentation and implementation of each applicable control.

The compliance thresholds depend on the assurance level. If these thresholds are not met, the entity should establish realistic remediation measures, internal owners and clear deadlines, so that the compliance process can be properly monitored and evidenced. The self-assessment is carried out in the NIS2@RO Platform or, temporarily, through the local tools EVAL_MMS_B, EVAL_MMS_I and EVAL_MMS_E, which generate the report that must be submitted to DNSC.

Who is exempted, and from what?

Order No. 1/2026 also amends, as mentioned above, the risk assessment methodology, clarifying the applicable exemptions.

Certain entities in the banking, financial market infrastructure, digital infrastructure and B2B ICT services sectors are exempted from the national risk assessment, to the extent that they fall within the scope of DORA.

Note! The exemption does not automatically apply to all entities in the sectors concerned and does not represent a general exemption from NIS 2. From this perspective, the recommendation is that the applicability of the exemption be rigorously verified on a case-by-case basis, depending on the entity's status, the activities carried out and the applicable sector-specific regulations.

Final considerations

With DNSC Order No. 1/2026, the companies concerned now have a clear standard against which to assess themselves when establishing and implementing the cybersecurity measures they are required to apply.

NIS2 compliance must be organised and budgeted internally so that the applicable deadlines and requirements are met effectively, coherently and in a documented manner. It should be viewed as a phased process, not as a mere formal exercise: risk assessment, determining the assurance level and applicable controls, self-assessment of maturity, submission of reports to DNSC and monitoring the launch of the NIS2@RO Platform must be integrated into a **clear and duly assumed internal calendar**.

Voicu & Asociații has set up a practice group dedicated to NIS2 implementation and is ready to assist the entities concerned in the procedures required to comply with the regulatory framework, leveraging the experience accumulated, including in the earlier stages of the applicable legislation, and working, on a case-by-case basis, with cybersecurity specialists for a comprehensive, 360° compliance process.

The information provided above is general and should not be considered legal advice for analysing and resolving a specific legal matter. If you have questions regarding a particular situation, please contact: **Voicu & Asociatii SCA**, office@voicu-asociatii.ro or by telephone at +4021 314 02 00.

VOICU
ASOCIAȚII
Attorneys at Law