

Does NIS2 apply to your company?

Three checks based on Romania's Emergency Ordinance (OUG) 155/2024, in its applicable consolidated form. Applicability depends on the entity type and activity listed in the annex, not just the general industry name.

1 Do you operate in one of the 18 sectors?

ANNEX 1 · SECTORS OF HIGH CRITICALITY

- ☐ Energy (electricity, district heating and cooling, oil, gas, hydrogen)
- ☐ Transport (air, rail, water; road transport covers road authorities and intelligent transport system operators)
- ☐ Banking (see DORA note)
- ☐ Financial market infrastructures (see DORA note)
- ☐ Health (healthcare, pharmaceutical production and distribution, pharmacies)
- ☐ Drinking water
- ☐ Waste water
- ☐ Digital infrastructure (DNS, TLD, cloud, data centres, electronic communications, trust services)
- ☐ Managed ICT services (including managed security services)
- ☐ Central public administration
- ☐ Space

ANNEX 2 · OTHER CRITICAL SECTORS

- ☐ Postal and courier services
- ☐ Waste management (where this is the principal activity)
- ☐ Chemicals (manufacture, production, distribution)
- ☐ Food (industrial production and processing, wholesale distribution)
- ☐ Manufacturing (medical devices, electronics and optical products, electrical equipment, machinery, vehicles and other transport equipment)
- ☐ Digital providers (online marketplaces, search engines, social networking platforms)
- ☐ Research

Basis: Annexes 1 and 2 to OUG 155/2024

Road transport: other company activities or circumstances may separately trigger inclusion. **DORA note:** for financial entities subject to DORA, ICT risk obligations are assessed under the special sectoral regime. Listing in a NIS2 annex does not mean full, cumulative application of the same obligations. Identification and registration obligations are checked separately.

2 Do you meet the statutory size criteria?

Headcount is not the only criterion. Fewer than 50 employees does not automatically mean exclusion. Check the legal thresholds, rules for partner/linked enterprises and categories covered regardless of size.

- ☐ **Medium-sized:** 50–249 employees and turnover of no more than EUR 50 million or assets of no more than EUR 43 million.
- ☐ **Covered regardless of size:** for example, central public administration, DNS services, TLD name registries and trust services. This list is not exhaustive.
- ☐ **Large:** above the medium-sized enterprise thresholds.

Basis: Arts. 5–9, OUG 155/2024; Art. 4, Law 346/2004

3 Do you have customers in these sectors?

- ☐ We supply products or services to entities in the sectors in step 1 (IT, software, maintenance, logistics, consultancy, or any service with access to their systems or data)

Covered entities must manage security risks associated with direct suppliers and service providers, and may impose contractual requirements proportionate to risk (Arts. 11 and 13, OUG 155/2024).

HOW TO READ THE RESULT

Annex 1 sector and large enterprise; central public administration, DNS services, TLD registries, qualified trust services

Most likely an essential entity
Art. 5

Annex 1 sector and medium-sized enterprise; Annex 2 sector and medium-sized or large enterprise

Most likely an important entity
Exceptions apply: some categories are essential even if medium-sized or regardless of size, including managed security service providers (MSSPs). Final classification is checked under Arts. 5–9 of OUG 155/2024.

Only step 3 applies

If you do not independently meet the direct applicability criteria, covered customers may still impose contractual security requirements. Supplier status alone does not establish NIS2 applicability.

Obligations timeline

Deadlines start from different events for each entity. First establish where you are on this path.

DEADLINE	OBLIGATION	STARTING POINT AND REQUIREMENTS	BASIS
30 days	Notification for registration	Submit within 30 days of the date on which the entity becomes subject to the applicable provisions.	Art. 18(2)
30 days	Appointment of the person responsible for security	From notification of the registration decision, subject to the conditions for the role and entity category. An IT support contract does not, by itself, constitute the statutory appointment.	Art. 14(3)–(4)
60 days	Submission of the risk-level assessment	For entities subject to this procedure: from notification of the registration decision. The resulting assurance level differs from the legal status of important or essential entity.	Art. 18(6)
60 days	Initial maturity self-assessment	Prepare and submit within the statutory 60-day period following submission of the risk-level assessment.	Art. 18(7)
30 days	Submission of the remediation plan	Essential entities submit the plan within 30 days of the self-assessment. This is the deadline for submitting the plan, not for completing all remediation.	Art. 12(5)
Annually	Periodic self-assessment	Performed annually, endorsed by management and submitted under the applicable procedure.	Art. 12(4)
24 h · 72 h	Reporting a significant incident	Early warning within 24 hours and incident notification within 72 hours, both from becoming aware. Final report within one month of incident notification, with special rules for ongoing incidents. Interim report at the authority's request; a special deadline applies to trust service providers.	Art. 15(7)–(8)

BEYOND FORMALITIES

Measures go beyond registration

Registration and self-assessment do not replace implementation: risk management, access and system security, incident management, continuity, backups, supplier security, training and checks of control effectiveness.

Basis: Arts. 11 and 13, OUG 155/2024

FOR THE MANAGEMENT MEETING

Five questions to ask

- ☐ Do we know, in writing, whether we are an essential entity, important entity or only a supplier?
- ☐ Have we submitted the registration notification and received the registration decision?
- ☐ Who is responsible for security, and to whom do they report?
- ☐ Can we prove we do what our policies say?
- ☐ Does someone know what to do in the first 24 hours after an incident?

ART. 60 OF OUG 155/2024

What the law provides

- **Administrative breaches:** certain breaches, including failure to meet registration obligations, attract the penalties for the acts listed in Art. 60. The cap depends on the breach and entity category.
- **Maximum cap:** for breaches subject to these limits, the higher of the fixed amount and the statutory percentage of total worldwide annual turnover in the preceding financial year: EUR 7 million or 1.4% for important entities; EUR 10 million or 2% for essential entities. The fine is determined in accordance with the law.
- **Management** approves and oversees the measures and has training obligations. It is liable, under the conditions laid down by law, for breaches of its duties (Art. 14).

REMEMBER

Self-assessment covers documentation and actual implementation. For certain digital providers and managed services, also check Implementing Regulation (EU) 2024/2690.

Need a reasoned applicability assessment?

Clarified IT prepares your applicability record, with a reasoned conclusion, obligations and a preliminary timeline.

it.clarified.ro/nis2

office@clarified.ro · +40 774 456 127

Sources: OUG 155/2024, approved with amendments and additions by Law 124/2025, in its applicable consolidated form; Directive (EU) 2022/2555; Regulation (EU) 2022/2554 (DORA); Law 346/2004. This checklist is informational: it offers guidance based on available information and does not replace assessment of the specific situation or the authority's decision or powers.