

Preparing for the NIS2 assessment

Guide for management and IT • Accompanies the Excel workbook with selectable answers

This material supplements the initial checklist, ‘Does NIS2 apply to your company?’, which remains unchanged. It helps us understand the scope, responsibilities and known situation before an assessment or audit. We do not ask you to carry out technical investigations in order to answer.

What you obtain at this stage

A declared view of the situation, the information that needs clarification and a basis for selecting the appropriate service. It does not result in an official DNSC score, a certificate or confirmation of compliance.

How to complete the file

WHO	WHERE TO COMPLETE	WHAT IT INDICATES
Request coordinator	01_Profile and 05_Deadlines	The entity, approximate volumes, contact roles and known stages.
Management / appointed person	02_Management — 14 questions	Responsibilities, critical activities, risks, decisions and resources.
Internal IT, IT provider or group	03_IT — 24 questions; 04_Special_Cases — 6	Existence of measures, scope covered and any unknowns.

Indicative time: 10–15 minutes for management and 15–25 minutes for IT, plus the profile data. These are estimates, not imposed deadlines. One copy is completed for each legal entity.

Five answers, without lengthy technical explanations

Yes — the situation is known for the entire relevant scope. Partially — it covers only part of the scope. No — according to the information known, the measure does not exist. Unknown — the information cannot be confirmed. Possibly not applicable — explain why; applicability will be validated later.

Complete only the pale-yellow cells. For ‘Yes’, evidence is reviewed later. For ‘Possibly not applicable’, the explanation does not constitute a legal exclusion. The summary counts answers; it does not calculate a compliance percentage.

What we clarify before the assessment

The questionnaire separates management decisions from technical execution. A company is not assumed compliant merely because it holds a licence, nor is a provider assumed to have taken over every management obligation. [R1–R3]

FUNCTION	CORE QUESTION	GUIDANCE EXAMPLES
Govern — GV	Who decides and monitors?	Responsibilities, policies, risk, suppliers, budget and reporting.
Identify — ID	What must be protected?	Known assets and applications, critical activities, vulnerabilities and dependencies.
Protect — PR	What reduces risk?	Access, authentication, devices, data, training, backups and segmentation.
Detect — DE	Who notices problems?	Alerts, logs, event monitoring and the actual monitoring schedule.
Respond — RS	What do we do during an incident?	Escalation, decisions, limiting impact, communication and preservation of evidence.
Recover — RC	How do we resume work?	Tested restoration, recovery priorities and alternative channels.

The six functions are taken from the structure of the DNSC measures. The questions are our own synthesis, not a reproduction of the catalogue or a substitute for checking all applicable controls. [R3]

Examples of an appropriate level of detail

For authentication: ‘Yes, for IT administrators; unknown for everyone else.’ For backup: ‘We have backups, but we do not know when restoration was last tested.’ For a group: ‘Security is managed centrally; the local responsible person can identify who confirms coverage.’

Do not send exploitable information or customer data

Do not enter passwords, tokens, keys, IP addresses, configurations, user lists, system extracts or vulnerability reports. Only the existence of measures and the role that can confirm them are requested.

Special areas — development, cloud, managed services, OT/IoT/medical, public exposure and the physical environment — are clarified separately. For DORA and digital categories covered by Regulation 2024/2690, the applicable regime is checked without assuming full cumulative application of the obligations. [R6]

Services that may follow

The proposal is prepared after the scope and identified need are understood. The pre-audit is a commercial preparation stage, not a separate universal obligation. A customer may need to proceed directly to an audit or may only need to complete certain evidence.

STAGE	WHAT IS DONE	CONCRETE RESULT
P1 • Initial assessment / pre-audit	Applicability, risk, documents and implementation; interviews and authorised checks. Preparing the self-assessment under the applicable procedure.	Situation report, gaps, evidence and support for the documents that must be endorsed/submitted.
P2 • Independent audit	Regulated audit performed by an independent DNSC-attested auditor; tools, documents, interviews and tests within the approved scope.	Audit report and findings. A scan alone does not constitute the audit.
P3 • Plan and budget	Risk-based prioritisation, treatment options, owners, deadlines, dependencies and initial/recurring costs.	Endorsed plan and transparent budget; preparation for submission where required.
P4 • Implementation	Technical and organisational solutions, configuration, training, acceptance tests and evidence collection.	Implemented and verified measures; documented limitations and residual risks.
P5 • Maintenance and reporting	Reviews and retesting, documentation updates, support for reassessments and applicable communications.	Current evidence and management reports; support for closing measures.

What the proposal must contain

The entities, sites and systems included; services and methods; number of interviews and checks; deliverables; access limits; assumptions; customer responsibilities; initial and recurring costs; exclusions; acceptance criteria; and conditions for changing the scope.

We start from the existing measures. Depending on risk, a requirement may be addressed by configuration, a procedure, training or a product. Choosing a brand is not, by itself, a condition of compliance.

We keep the services separate

The customer is not required to purchase every stage from the same provider. Implementation and the independent audit have distinct roles. Licences, hardware and special operations are defined separately in the proposal.

How the technical verification is carried out

A tool may assist with inventory and with checking certain configurations, permissions, vulnerabilities or logs, according to its actual capabilities. By itself, it cannot demonstrate governance, risk acceptance, application of every procedure or full fulfilment of the requirements.

Before any connection

ITEM	WHAT WE AGREE IN WRITING
Scope and method	Systems included/excluded, collection method, approved scans/tests, time windows and stop rules.
Access and changes	Minimum privileges; read-only access where the method allows; controlled accounts revoked after the work. Changes require separate approval.
Data and confidentiality	Data collected, storage location, recipients, retention period and deletion. Confidentiality and processing agreements, where appropriate.
Third parties and sensitive systems	Permission from owners/providers; a safe method and approved windows for OT, medical and critical systems. No active scanning by default.
Delivery and traceability	Activity log, findings, relevant evidence, tool limitations and matters requiring manual verification.

The questionnaire does not authorise scanning

Selecting 'I would like a proposal' or returning the Excel workbook does not constitute consent for access, installation of an agent, system scanning or configuration changes.

Who is responsible and who verifies

Management approves and monitors the measures, provides resources and assumes the applicable obligations. The assessment/implementation team carries out the agreed mandate. The attested auditor independently formulates the conclusions of the regulated audit. [R1–R2]

Independence is also checked where the auditor and implementer belong to different companies in the same group: current and previous services, professional/financial relationships and the incompatibilities under Article 58 are examined. The mere existence of two companies is not sufficient. [R2]

We do not promise an auditor's 'authorisation' of the self-assessment and do not present the tool as issuing NIS2 certification. Roles, attestations and any recognitions are checked in practice before contracting.

From findings to implementation and reporting

A useful plan is not a product list. Each finding must be linked to a requirement, evidence, the risk to the business and a criterion that demonstrates remediation.

IN THE PLAN	WHAT MUST BE CLEAR
Finding and risk	What was checked, what the gap is, which activity may be affected and why it has a particular priority.
Options and costs	What can be resolved with existing solutions; alternatives; initial cost, recurring cost and estimation assumptions.
Owner and deadline	Who is accountable internally, who implements, dependencies, required downtime and the agreed deadline.
Acceptance and evidence	The test to be performed, evidence retained, the person who accepts it and the residual risk still requiring treatment.
Communication	The document submitted, applicable basis/deadline, management endorsement and evidence of communication to the authority.

The timeline is established for each entity

The initial checklist and 05_Deadlines record the milestones: registration, decision, risk assessment, self-assessment, plan and audit. The deadline for submitting the plan after self-assessment is separate from the implementation deadline and the route for the audit plan. Articles 12, 18 and 57 of the Ordinance are checked separately. [R2]

Compliance does not follow merely from filing a document. Assistance with submitting the plan or communicating completion of the measures is based on a mandate, the obligation that actually applies and evidence. Incomplete measures are not declared complete; blockers and revised deadlines are addressed under the applicable framework.

Incidents do not wait for the project to finish

The operating procedure must account for reporting significant incidents: warning within 24 hours and notification within 72 hours of becoming aware, followed by a final report and any updates within the applicable deadlines, subject to the statutory exceptions. [R1–R2]

What we receive back now

Only the completed Excel workbook, with the known information and the people/roles who can confirm it. We then establish the clarifications, scope and proposal. Supporting documents and technical access are requested later, through a secure channel and within the agreed limits.

Basis and limitations of this material

The received CSAT/CISv8 technical questionnaire contains 63 questions across 20 topics. These were grouped thematically into 44 questions in Romanian and supplemented with areas from the NIS2/DNSC framework. The internal register retains the original questions, their location in Excel and the working mappings.

The Basic, Standardized, Rationalized and Dynamic scales, the Risk values and the source's commercial product recommendations were not converted into DNSC scores, budgets or purchasing obligations. A 'Yes' is a statement to be verified, not evidence. A 'Possibly not applicable' response does not, by itself, establish or approve a legal exclusion.

Normative references

REF.	SOURCE AND USE
R1	Directive (EU) 2022/2555: Articles 20 (management), 21 (cybersecurity risk-management measures), 23 (incidents). EUR-Lex: CELEX 32022L2555.
R2	Government Emergency Ordinance no. 155/2024, approved with amendments by Law no. 124/2025, consolidated form: Articles 11–15, 18, 57–58 and the annexes. Romanian Legislative Portal: document 293121.
R3	DNSC Order no. 1/2026, published on 27 August 2026, annexes concerning the measures and self-assessment. Romanian Legislative Portal: documents 314681 / 314360 / 314683.
R4	DNSC Order no. 2/2026: amendments to the framework concerning non-applicability and group controls. Romanian Legislative Portal: document 314676.
R5	DNSC Decision no. 3/2026 and the rules for groups: application and local evidence, responsibilities. Romanian Legislative Portal: documents 314698 / 314699.
R6	Regulation (EU) 2022/2554 — DORA and Implementing Regulation (EU) 2024/2690, within their respective scopes. EUR-Lex: CELEX 32022R2554 / 32024R2690.

The complete addresses and the role of each source are in the 08_References sheet in Excel. Package reference date: 6 October 2026. The legislation and procedures applicable on the date of the entity's assessment must be used.

Terms, briefly

MFA: confirming access through more than one factor. OT: systems that control physical processes or equipment. Backup: a safety copy; its existence does not demonstrate restoration. Evidence: a document, record or test result that supports a finding. Residual risk: the risk remaining after measures.

Request coordination

Cristian Apostol • office@clarified.ro • +40 774 456 127
it.clarified.ro/nis2