

Pregătirea pentru evaluarea NIS2

Ghid pentru conducere și IT • Însoțește Excelul cu răspunsuri selectabile

Acest material completează fișa inițială „Intră firma ta sub NIS2?”, care rămâne neschimbată. Ne ajută să înțelegem perimetrul, responsabilitățile și situația cunoscută, înainte de o evaluare sau de un audit. Nu vă cerem să efectuați investigații tehnice pentru a răspunde.

Ce obțineți în această etapă

O imagine declarată a situației, informațiile de clarificat și o bază pentru stabilirea serviciului potrivit. Nu rezultă un scor oficial DNSC, un certificat sau confirmarea conformității.

Cum completați fișierul

Cine	Unde completează	Ce indică
Coordonatorul solicitării	01_Profil și 05_Termene	Entitatea, volume aproximative, rolurile de contact și stadiile cunoscute.
Conducerea / persoana desemnată	02_Conducere — 14 întrebări	Responsabilități, activități critice, riscuri, decizii și resurse.
IT intern, furnizorul IT sau grupul	03_IT — 24 întrebări; 04_Speciale — 6	Existența măsurilor, aria acoperită și eventualele necunoscute.

Timp orientativ: 10–15 minute pentru conducere și 15–25 minute pentru IT, plus datele de profil. Sunt estimări, nu termene impuse. O copie se completează pentru fiecare entitate juridică.

Cinci răspunsuri, fără explicații tehnice lungi

Da — situația este cunoscută pentru întregul perimetru relevant. Parțial — acoperă doar o parte. Nu — măsura nu există, potrivit informațiilor cunoscute. Nu știm — informația nu poate fi confirmată. Posibil neaplicabil — explicați motivul; aplicabilitatea se validează ulterior.

Completați numai celele galben-pal. La „Da”, dovezile se examinează ulterior; la „Posibil neaplicabil”, explicația nu constituie o excludere legală. Rezumatul numără răspunsurile, nu calculează un procent de conformitate.

Ce clarificăm înainte de evaluare

Chestionarul separă decizia managerială de execuția tehnică. Nu presupune că o firmă este conformă pentru că are o anumită licență sau că un furnizor a preluat automat toate obligațiile conducerii. [R1–R3]

Funcție	Întrebarea de fond	Exemple de orientare
Guvernare — GV	Cine decide și urmărește?	Responsabilități, politici, risc, furnizori, buget și raportare.
Identificare — ID	Ce trebuie protejat?	Active și aplicații cunoscute, activități critice, vulnerabilități și dependențe.
Protecție — PR	Ce reduce riscul?	Acces, autentificare, dispozitive, date, instruire, copii de siguranță și segmentare.
Detecție — DE	Cine observă problemele?	Alerte, jurnale, urmărirea evenimentelor și programul real de monitorizare.
Răspuns — RS	Ce facem la incident?	Escaladare, decizii, limitarea efectelor, comunicare și păstrarea dovezilor.
Recuperare — RC	Cum reluăm activitatea?	Restaurare testată, priorități de reluare și comunicații alternative.

Cele șase funcții sunt preluate din structura măsurilor DNSC. Întrebările sunt o sinteză proprie, nu reproducerea catalogului și nu un substitut pentru verificarea tuturor controalelor aplicabile. [R3]

Exemple de nivel de detaliu potrivit

Pentru autentificare: „Da, pentru administratorii IT; nu știm pentru ceilalți”. Pentru backup: „Avem copii de siguranță, dar nu știm când s-a testat restaurarea”. Pentru grup: „Securitatea este gestionată central; responsabilul local poate indica persoana care confirmă acoperirea”.

Nu trimiteți informații exploatabile sau date ale clienților

Nu introduceți parole, tokenuri, chei, adrese IP, configurații, liste de utilizatori, extrase din sisteme sau rapoarte de vulnerabilități. Se solicită doar existența măsurilor și rolul care le poate confirma.

Domeniile speciale — dezvoltare, cloud, servicii gestionate, OT/IoT/medical, expunere publică și mediu fizic — se clarifică separat. Pentru DORA și categoriile digitale vizate de Regulamentul 2024/2690 se verifică regimul aplicabil, fără a presupune cumularea integrală a obligațiilor. [R6]

Serviciile care pot urma

Propunerea se construiește după perimetrul și nevoia constatată. Preauditul este o etapă comercială de pregătire, nu o obligație distinctă universală. Un client poate avea nevoie direct de audit sau numai de completarea unor dovezi.

Etapă	Ce se face	Rezultat concret
P1 • Evaluare inițială / preaudit	Încadrare, risc, documentație și implementare; interviuri și verificări autorizate. Pregătirea autoevaluării în procedura aplicabilă.	Raport de situație, diferențe, dovezi și suport pentru documentele care trebuie asumate/transmise.
P2 • Audit independent	Audit reglementat efectuat de auditor atestat DNSC, independent; tool-uri, documente, interviuri și teste în perimetrul aprobat.	Raport de audit și constatări. O scanare nu reprezintă singură auditul.
P3 • Plan și buget	Prioritizare pe risc, opțiuni de tratare, responsabili, termene, dependențe și costuri inițiale/recurente.	Plan asumat și buget transparent; pregătirea transmiterii unde este cerută.
P4 • Implementare	Soluții tehnice și organizaționale, configurare, instruire, teste de acceptanță și colectarea dovezilor.	Măsurile implementate și verificate; limite și riscuri reziduale consemnate.
P5 • Menținere și raportare	Revizuirii și retestări, actualizarea documentației, sprijin pentru reevaluări și comunicările aplicabile.	Dovezi actualizate și rapoarte pentru conducere; suport pentru închiderea măsurilor.

Ce trebuie să conțină oferta

Entitățile, sediile și sistemele incluse; serviciile și metodele; numărul de interviuri și verificări; livrabilele; limitele de acces; ipotezele; responsabilitățile clientului; costurile inițiale și recurente; excluderile; criteriile de acceptanță și condițiile de schimbare a perimetrului.

Pornim de la măsurile existente. O cerință poate fi acoperită prin configurare, procedură, instruire sau produs, după risc. Alegerea unei mărci nu este, prin ea însăși, o condiție de conformare.

Păstrăm delimitarea între servicii

Clientul nu este obligat să achiziționeze toate etapele de la același prestator. Implementarea și auditul independent au roluri distincte. Licențele, hardware-ul și operațiunile speciale se delimitează în ofertă.

Cum se desfășoară verificarea tehnică

Un instrument poate ajuta la inventariere și la verificarea unor configurații, drepturi, vulnerabilități sau jurnale, în funcție de capabilitățile sale reale. Nu poate demonstra singur guvernanta, acceptarea riscurilor, aplicarea tuturor procedurilor sau îndeplinirea integrală a cerințelor.

Înainte de orice conectare

Element	Ce convenim în scris
Perimetru și metodă	Sistemele incluse/excluse, tipul de colectare, scanările/testele aprobate, intervalele și regulile de oprire.
Acces și modificări	Drepturi minime; acces numai în citire unde metoda permite; conturi controlate și revocate după lucru. Modificările cer aprobare distinctă.
Date și confidențialitate	Datele colectate, locul de stocare, destinarii, durata de păstrare și ștergerea. Acordurile de confidențialitate și de prelucrare, după caz.
Terți și sisteme sensibile	Permisiunea proprietarilor/furnizorilor; pentru OT, medical și sisteme critice, metodă sigură și ferestre aprobate. Fără scanare activă implicită.
Livrare și trasabilitate	Jurnalul intervențiilor, constatările, probele relevante, limitările instrumentului și ce necesită verificare manuală.

Chestionarul nu autorizează scanarea

Selectarea „Doresc o propunere” sau returnarea Excelului nu înseamnă acord pentru acces, instalarea unui agent, scanarea sistemelor sau schimbarea configurațiilor.

Cine răspunde și cine verifică

Conducerea aprobă și urmărește măsurile, asigură resursele și își asumă obligațiile aplicabile. Echipa de evaluare/implementare execută mandatul convenit. Auditorul atestat formulează independent concluziile auditului reglementat. [R1–R2]

Independența se verifică inclusiv când auditorul și implementatorul aparțin unor firme diferite din același grup: se examinează serviciile curente și anterioare, relațiile profesionale/financiare și incompatibilitățile prevăzute de art. 58. Simplul fapt că există două societăți nu este suficient. [R2]

Nu promitem „autorizarea” autoevaluării de către un auditor și nu prezentăm tool-ul ca emitent al unei certificări NIS2. Rolurile, atestările și eventualele recunoașteri se verifică efectiv, înainte de contractare.

De la constatări la implementare și raportare

Un plan util nu este o listă de produse. Fiecare constatare trebuie legată de o cerință, de o probă, de riscul pentru activitate și de un criteriu prin care se demonstrează remedierea.

În plan	Ce trebuie să fie clar
Constatare și risc	Ce s-a verificat, care este diferența, ce activitate poate fi afectată și de ce are o anumită prioritate.
Opțiuni și costuri	Ce se poate rezolva cu soluțiile existente; alternative; cost inițial, cost recurent și ipotezele estimării.
Responsabil și termen	Cine răspunde intern, cine implementează, dependențele, indisponibilitatea necesară și termenul asumat.
Acceptanță și dovadă	Testul de efectuat, proba păstrată, persoana care acceptă și riscul rezidual care mai trebuie tratat.
Comunicare	Documentul transmis, temeiul/termenul aplicabil, asumarea conducerii și dovada comunicării către autoritate.

Calendarul se stabilește pentru fiecare entitate

Fișa inițială și fila 05_Termene colectează reperele: înregistrare, decizie, evaluarea riscului, autoevaluare, plan și audit. Termenul de transmitere a planului după autoevaluare nu se confundă cu termenul de implementare și nici cu traseul planului rezultat din audit. Se verifică distinct art. 12, art. 18 și art. 57 din OUG. [R2]

Conformitatea nu rezultă din simpla depunere a unui document. Asistența la transmiterea planului sau la comunicarea îndeplinirii măsurilor se bazează pe mandat, pe obligația efectiv aplicabilă și pe dovezi. Măsurile nefinalizate nu se declară îndeplinite; blocajele și termenele revizuite se tratează potrivit cadrului aplicabil.

Incidentele nu așteaptă finalizarea proiectului

Procedura operațională trebuie să țină cont de raportarea incidentelor semnificative: avertizare în 24 de ore și notificare în 72 de ore de la luarea la cunoștință, apoi raport final și eventuale actualizări în termenele aplicabile, cu excepțiile legale. [R1–R2]

Ce primim înapoi acum

Numai Excelul completat, cu informațiile cunoscute și persoanele/rolurile care le pot confirma. Stabilim apoi clarificările, perimetrul și propunerea. Documentele justificative și accesul tehnic se cer ulterior, pe canal securizat și în limitele convenite.

Baza materialului și limitele sale

Chestionarul tehnic CSAT/CISv8 primit conține 63 de întrebări în 20 de teme. Acestea au fost agregate tematic în 44 de întrebări în limba română și completate cu domenii din cadrul NIS2/DNSC. Registrul intern păstrează întrebările originale, localizarea în Excel și asocierile de lucru.

Scările Basic, Standardized, Rationalized și Dynamic, valorile Risk și recomandările comerciale de produse din sursă nu au fost transformate în scoruri DNSC, bugete sau obligații de achiziție. Un „Da” este o declarație de verificat, nu o probă. Un „Posibil neaplicabil” nu consumă și nu aprobă o excludere legală.

Repere normative

Ref.	Sursă și utilizare
R1	Directiva (UE) 2022/2555: art. 20 (conducere), 21 (măsurile de gestionare a riscurilor), 23 (incidente). EUR-Lex: CELEX 32022L2555.
R2	OUG nr. 155/2024, aprobată cu modificări prin Legea nr. 124/2025, forma consolidată: art. 11–15, 18, 57–58 și anexele. Portalul Legislativ: document 293121.
R3	Ordinul DNSC nr. 1/2026, publicat la 27.08.2026, anexele privind măsurile și autoevaluarea. Portalul Legislativ: documente 314681 / 314360 / 314683.
R4	Ordinul DNSC nr. 2/2026: modificări ale cadrului privind neaplicabilitatea și controalele de grup. Portalul Legislativ: document 314676.
R5	Decizia DNSC nr. 3/2026 și normele pentru grupuri: aplicare și dovezi locale, responsabilități. Portalul Legislativ: documente 314698 / 314699.
R6	Regulamentul (UE) 2022/2554 — DORA și Regulamentul de punere în aplicare (UE) 2024/2690, în domeniile lor de aplicare. EUR-Lex: CELEX 32022R2554 / 32024R2690.

Adresele complete și rolul fiecărei surse sunt în fila 08_Referinte din Excel. Data de referință a pachetului: 6 octombrie 2026. Se utilizează actele și procedurile aplicabile la data evaluării entității.

Termeni, pe scurt

MFA: confirmarea accesului prin mai mult de un factor. OT: sisteme care comandă procese sau echipamente fizice. Backup: copie de siguranță; existența ei nu dovedește restaurarea. Dovadă: document, înregistrare sau rezultat de test care susține o constatare. Risc rezidual: riscul care rămâne după măsuri.

Coordonarea solicitării

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