PRODEFENCE

SECURITATE • CONFORMITATE • REZILIENȚĂ

NIS 2.0

GHID PRACTIC

Primii pași în NIS2

Ghid de referință pentru identificare, notificare, evaluare de risc, implementare, audit și raportare în relația cu DNSC

Flux operațional aliniat cu Directiva (UE) 2022/2555, OUG nr. 155/2024, Legea nr. 124/2025 și ordinele Directoratului Național de Securitate Cibernetică aplicabile



- Conformitate legală
- Abordare structurată
- Risc redus și controlat
- Reziliență operațională
- Încredere și continuitate

Pentru management, IT, securitate, juridic, achiziții, operațional, audit intern și responsabili de conformitate

HTTPS://WWW.PRODEFENCE.RO/

Disclaimer și limite de utilizare

Ghidul are caracter informativ și operațional. Documentul nu înlocuiește consultanța juridică, analiza individuală a fiecărei organizații, deciziile Directoratului Național de Securitate Cibernetică sau instrucțiunile oficiale emise de autoritățile competente.

Organizațiile trebuie să verifice permanent forma actualizată a actelor normative, instrucțiunile publicate de DNSC și cerințele sectoriale aplicabile. Informațiile din acest ghid sunt structurate pentru a sprijini o abordare practică, proporțională și documentabilă a conformării NIS2 în România.

Principiu de utilizare

Ghidul trebuie folosit ca instrument de orientare, planificare și control intern. Încadrarea finală, obligațiile concrete, termenele și măsurile aplicabile trebuie determinate pe baza datelor reale ale organizației și a cadrului reglementar în vigoare.

Autorul ghidului: Alexandru Angheluș

Cuprins

Disclaimer și limite de utilizare 1
1. Mesaj pentru management 4
2. Cui se adresează ghidul 4
3. Cadrul legal și operațional de referință 5
4. Termeni esențiali și principii de lucru 5
Principii de lucru 6
5. Fluxul DNSC pe scurt 6
6. Fluxul DNSC detaliat cu livrabile 7
6.1 Decizia internă și echipa NIS2 7
6.2 Colectarea datelor pentru identificare 7
6.3 Utilizarea Platformei NIS2@RO / Instrumentului NIS2@RO 7
6.4 Evaluarea gradului de perturbare, dacă este aplicabilă 7
6.5 Transmiterea notificării către DNSC 8
6.6 Evaluarea DNSC și decizia privind înregistrarea 8
6.7 Evaluarea nivelului de risc 8
6.8 Stabilirea cerințelor aplicabile și matricea de conformitate 9
6.9 Planul de implementare 9
6.10 Implementarea măsurilor 9
6.11 Documente și dovezi 10
6.12 Autoevaluarea maturității 10
6.13 Planul de remediere 10
6.14 Audit și pregătire pentru control 10
6.15 Raportare incidente și cooperare continuă 11
7. Checklist de pregătire pentru notificarea DNSC 11
8. Model de dosar NIS2 12
9. RACI extins de responsabilități 12
10. Documente și registre minime recomandate 13
10.1 Documente pentru inițiere și notificare 13
10.2 Documente pentru implementare 13
10.3 Registre operaționale recomandate 13
10.4 Documente pentru audit și control 14
11. Matrice operațională Art. 21: cerințe, controale, dovezi 14
12. Roadmap de implementare 30/60/90 zile și calendar anual 15
Calendar anual minim recomandat 15
13. Managementul riscurilor: registru, tratament, risc rezidual 15
14. Playbook pentru incidente și raportare 16
Model minim de registru incidente 16
15. Managementul furnizorilor și lanțului de aprovizionare 17
Clauze contractuale recomandate pentru furnizori critici 17

16. Audit, autoevaluare și pregătire pentru control 17
Pachet minim pentru audit/preaudit 18
17. Ce trebuie să știe conducerea 18
Raport lunar recomandat către conducere 18
18. Greșeli frecvente și cum se evită 18
19. Cum ajută platforma CysNis 19
20. Contractarea unui consultant Prodefence 20
20.1 Când este recomandat consultantul 20
20.2 Ce poate livra consultantul Prodefence 20
20.3 Livrabile contractuale 20
21. Responsabil NIS2 extern prin Prodefence 20
21.1 Când este util 21
21.2 Ce face responsabilul NIS2 extern 21
22. Mini-studii de caz 21
22.1 Organizație de producție cu furnizori digitali critici 21
22.2 Spital sau furnizor de servicii medicale 21
22.3 Furnizor digital / serviciu cloud sau SaaS 22
23. Checklist final de autoverificare 22
24. Modele și anexe operaționale 22
24.1 Model: Decizie internă de demarare NIS2 23
24.2 Model: Fișă serviciu relevant NIS2 23
24.3 Model: Raport lunar NIS2 către management 23
24.4 Model: Lista documentelor pentru proiect NIS2 23
24.5 Model: Criterii interne de clasificare a constatărilor 24
25. Referințe normative și bibliografie 24

1. Mesaj pentru management

Directiva NIS2 nu este doar o obligație tehnică pentru departamentul IT. Este un cadru de guvernanță, management al riscurilor, continuitate operațională, securitate a lanțului de aprovizionare și raportare, cu impact direct asupra conducerii organizației.

Pentru organizațiile din România, fluxul corect trebuie să urmeze logica reglementată de DNSC: identificare, notificare, evaluare, înregistrare, stabilire nivel de risc, aplicare măsuri, autoevaluare, remediere, audit și raportare continuă a incidentelor.

Mesaj-cheie pentru management

Nu începeți cu documentele și nu începeți cu checklistul. Începeți cu identificarea corectă, notificarea fundamentată, evaluarea riscului și stabilirea nivelului de măsuri aplicabil.

Scopul acestui ghid este să ofere o ordine de lucru aplicabilă, livrabile clare și un set de instrumente minime pentru organizațiile care trebuie să demonstreze că au un proces real de conformare NIS2, nu doar o colecție de politici.

Întrebare de management	Răspuns operațional așteptat
Știm dacă intrăm în NIS2?	Există fișă de identificare, sector/ subsector, servicii relevante, justificare și eventual notificare DNSC.
Știm ce risc avem?	Există evaluare de perturbare unde este aplicabilă, evaluare ENIRE@RO/mecanism DNSC și nivel de măsuri stabilit.
Știm ce trebuie implementat?	Există matrice de conformitate și plan de implementare aprobat.
Putem demonstra implementarea?	Există politici, proceduri, registre, rapoarte, dovezi tehnice, teste și aprobări.
Suntem pregătiți pentru incident/audit/control?	Există playbook incident, registru incidente, raportare, autoevaluare, preaudit și plan de remediere.

2. Cui se adresează ghidul

Ghidul este conceput pentru organizații care vor să înțeleagă primii pași practici în NIS2 și relația cu DNSC, dar și pentru organizații care au început implementarea și au nevoie de o structură de referință pentru consolidare.

- conducere executivă, administratori, directori generali și membri ai consiliilor de administrație;
- responsabili IT, securitate cibernetică, CISO/ vCISO și responsabili NIS2;
- departamente juridice, conformitate, achiziții, operațional, resurse umane și audit intern;
- entități publice, spitale, companii de utilități, transport, producție, furnizori digitali și organizații cu servicii critice;
- organizații care nu știu încă dacă intră sau nu în domeniul de aplicare NIS2;
- organizații deja înregistrate, care trebuie să transforme cerințele în măsuri, registre, dovezi și raportare.

Cum se folosește ghidul

Utilizați capitolele 5-6 pentru flux, capitolele 7-11 pentru livrabile și controale, capitolele 12-16 pentru implementare și audit, iar capitolul 24 ca set de modele operaționale.

3. Cadrul legal și operațional de referință

Fluxul descris în acest ghid are la bază cadrul european și național aplicabil NIS2 în România. Tabelul următor indică rolul operațional al principalelor acte normative, ordine DNSC și instrumente utilizate în practică.

Referință	Ce reglementează	De ce contează practic
Directiva (UE) 2022/2555 - NIS2	Stabilește cerințele europene pentru un nivel comun ridicat de securitate cibernetică.	Definește principiile de management al riscului, obligațiile de raportare, responsabilitatea conducerii și domeniile de măsuri.
OUG nr. 155/2024	Transpune NIS2 în spațiul cibernetic național civil.	Stabilește cadrul național, rolul DNSC, entitățile vizate, măsurile și obligațiile de raportare.
Legea nr. 124/2025	Aprobă și modifică OUG nr. 155/2024.	Consolidează cadrul național aplicabil entităților esențiale și importante.
Ordin DNSC nr. 1/2025	Reglementează cerințele privind notificarea în vederea înregistrării și metoda de transmitere a informațiilor.	Este reperul principal pentru notificarea către DNSC și înscrierea în registru.
Ordin DNSC nr. 2/2025	Reglementează criteriile/pragurile de perturbare și metodologia de evaluare a nivelului de risc.	Determină evaluarea perturbării și nivelul de măsuri aplicabile: bază, important sau esențial.
Ordin DNSC nr. 3/2025	Reglementează supravegherea, verificarea, controlul și prioritizarea pe bază de risc.	Este relevant pentru pregătirea organizației pentru audit, control și demonstrarea conformității.
CyFun® / ENIRE@RO / mecanisme DNSC	Instrumente și metodologii utilizate pentru maturitate, evaluare și nivel de risc.	Ajută la transformarea cerințelor în niveluri, controale, gap-uri și acțiuni concrete.

Atenție la actualizare

La publicarea sau utilizarea ghidului, verificați forma oficială actualizată a actelor normative și instrucțiunile DNSC. Acest document este un ghid operațional, nu o republicare a legislației.

4. Termeni esențiali și principii de lucru

Termen	Înțeles operațional în acest ghid
Entitate esențială / importantă	Organizație care intră în domeniul NIS2/OUG 155/2024 în funcție de sector, serviciu, dimensiune și criterii speciale.
Serviciu relevant NIS2	Serviciu prestat de organizație care se încadrează în anexele și criteriile cadrului național NIS2.
Perturbare	Întreruperea, afectarea confidențialității sau afectarea modului de funcționare a unui serviciu relevant.
Nivel de risc	Rezultatul evaluării prin metodologia/instrumentul aplicabil; determină nivelul de măsuri necesar.
Control	Măsură tehnică, operațională sau organizatorică implementată pentru reducerea riscului.
Dovadă	Document, registru, raport, log, captură, aprobare, test sau altă înregistrare care demonstrează implementarea.

Risc rezidual	Riscul rămas după implementarea măsurilor și acceptat sau tratat suplimentar de management.

Principii de lucru

- Proporționalitate: măsurile trebuie calibrate la nivelul de risc, dimensiunea și rolul organizației.
- Trasabilitate: fiecare cerință trebuie legată de un responsabil, un control și o dovadă.
- Dovezi înainte de declarații: nu se marchează „implementat” fără dovadă verificabilă.
- Management implicat: securitatea cibernetică este risc organizațional, nu doar problemă IT.
- Îmbunătățire continuă: conformarea NIS2 trebuie menținută prin revizuiri, audituri, exerciții și actualizări.

5. Fluxul DNSC pe scurt

Fluxul corect este ordinea reglementată și operațională prin care organizația își stabilește aplicabilitatea, transmite date către DNSC, primește sau clarifică încadrarea, evaluează nivelul de risc și implementează măsurile aplicabile.

Nr.	Etapă	Rezultat practic
1	Decizie internă și echipă NIS2	Mandat, factor decizional, responsabil, echipă și calendar.
2	Colectare date pentru identificare	Servicii, sector, dimensiune, sisteme, furnizori, dependențe.
3	Utilizare Platforma/ Instrument NIS2@RO sau ENIRE@RO CysNis	Introducere date, calificare, generare formular.
4	Evaluare perturbare, dacă este aplicabilă	Impact, praguri, justificări și dovezi pe serviciu.
5	Transmitere notificare DNSC	Formular semnat, transmis, dovadă și arhivare.
6	Evaluare DNSC și decizie	Clarificări, completări, înregistrare sau neîncadrare.
7	Evaluare nivel de risc	ENIRE@RO/ mecanism DNSC sau ENIRE@RO CysNis, scor, nivel de măsuri.
8	Matrice și plan	Cerințe, controale, responsabili, termene, dovezi.
9	Implementare măsuri	Art. 21/OUG 155: guvernanță, riscuri, incidente, continuitate, furnizori etc.
10	Documente și dovezi	Politici, proceduri, registre, rapoarte, teste, aprobări.
11	Autoevaluare, audit, remediere	Maturitate, gap-uri, audit/ preaudit, plan de acțiuni.
12	Raportare incidente continuă	Detectare, clasificare, notificare, lecții învățate.

Regula de bază

Platforma susține fluxul. Nu fluxul trebuie forțat după meniul platformei. CysNis trebuie folosit ca instrument de organizare, trasabilitate și urmărire a conformării, în ordinea impusă de logica DNSC.

6. Fluxul DNSC detaliat cu livrabile

6.1 Decizia internă și echipa NIS2

Conducerea decide inițierea procesului, stabilește factor decizionalul de management, responsabilul NIS2/ securitate și persoanele-cheie din IT, juridic, achiziții, operațional, HR și audit intern.

Livrabil	Descriere
Decizie internă de inițiere	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
RACI preliminar	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Calendar de proiect	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Dosar NIS2 deschis	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.

6.2 Colectarea datelor pentru identificare

Organizația colectează date despre servicii, sectoare, subsectoare, tipuri de entități, dimensiune, sedii, procese, sisteme informatice, furnizori și dependențe critice. Codul CAEN este doar un indiciu; serviciul furnizat și rolul real al entității sunt determinante.

Livrabil	Descriere
Fișă internă de identificare	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Listă servicii relevante	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Inventar inițial active și sisteme	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Listă furnizori critici	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.

6.3 Utilizarea Platformei NIS2@RO / Instrumentului NIS2@RO

Datele colectate sunt introduse în mecanismele DNSC pentru identificare, calificare și generarea formularului de notificare. Instrumentele DNSC trebuie tratate ca parte a fluxului formal, nu ca anexă administrativă.

Livrabil	Descriere
Formular de notificare generat	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Date validate intern	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Jurnal verificări și ipoteze	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.

6.4 Evaluarea gradului de perturbare, dacă este aplicabilă

Se analizează impactul perturbării serviciilor relevante: întrerupere, afectarea confidențialității sau afectarea modului de funcționare. Evaluarea trebuie corelată cu serviciile din anexele OUG nr. 155/2024.

Livrabil	Descriere
Fișe de perturbare pe serviciu	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Scenarii de impact	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Dovezi și justificări	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Aprobări interne	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.

6.5 Transmiterea notificării către DNSC

Formularul se semnează de reprezentantul legal sau reprezentanții legali și se transmite conform metodei aplicabile. Organizația trebuie să păstreze formularul, confirmarea, dovezile și comunicările ulterioare.

Livrabil	Descriere
Formular semnat	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Dovadă transmitere	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Registru comunicări DNSC	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Dosar notificare arhivat	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.

6.6 Evaluarea DNSC și decizia privind înregistrarea

DNSC poate solicita clarificări, completări sau documente justificative. După analiză, autoritatea poate decide înregistrarea ca entitate esențială/ importantă sau poate comunica neîncadrarea.

Livrabil	Descriere
Decizie/ confirmare DNSC	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Răspunsuri la clarificări	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Actualizare status intern	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.

6.7 Evaluarea nivelului de risc

După înregistrare, entitatea determină nivelul de risc prin mecanismele aplicabile, inclusiv ENIRE@RO. Nivelul de risc determină nivelul măsurilor tehnice, operaționale și organizatorice.

Livrabil	Descriere
Raport evaluare risc	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Scor general	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.

Nivel de măsuri	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Ipoteze și documente suport	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.

6.8 Stabilirea cerințelor aplicabile și matricea de conformitate

Cerințele legale și operaționale sunt transformate într-o matrice care leagă cerința, controlul, responsabilul, documentul, dovada, statusul, riscul și termenul.

Livrabil	Descriere
Matrice conformitate	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Lista controalelor aplicabile	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Prioritizare pe risc	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.

6.9 Planul de implementare

Planul se face după stabilirea nivelului de risc și a cerințelor aplicabile. El trebuie să includă măsuri, responsabili, termene, priorități, dependențe, buget și dovezi așteptate.

Livrabil	Descriere
Plan aprobat	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Roadmap 30/60/90 zile	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Indicatori de progres	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Raportare management	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.

6.10 Implementarea măsurilor

Se implementează măsuri de management al riscurilor, incidente, continuitate, backup, furnizori, dezvoltare și mentenanță, evaluare eficacitate, igienă cibernetică, instruire, criptografie, acces, active, MFA și comunicații securizate.

Livrabil	Descriere
Controale implementate	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Proceduri aplicate	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Dovezi tehnice	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Teste și exerciții	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.

6.11 Documente și dovezi

Documentele trebuie să reflecte modul real de lucru. Fiecare control trebuie susținut de politici, proceduri, registre, rapoarte, dovezi tehnice, aprobări sau evidențe operaționale.

Livrabil	Descriere
Dosar NIS2 auditabil	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Registru dovezi	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Control versiuni documente	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.

6.12 Autoevaluarea maturității

Organizația evaluează ce există, ce funcționează, ce este testat, ce este documentat și ce lipsește. Autoevaluarea trebuie să genereze acțiuni, nu doar un scor.

Livrabil	Descriere
Raport autoevaluare	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Gap-uri	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Plan de îmbunătățire	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.

6.13 Planul de remediere

Neconformitățile se transformă în acțiuni corective, cu responsabili, termene și dovezi de închidere. Managementul trebuie informat periodic.

Livrabil	Descriere
Plan remediere	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Dashboard progres	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Dovezi închidere	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.

6.14 Audit și pregătire pentru control

Auditul intern sau preauditul verifică documentele, controalele, dovezile și aplicarea practică. Pregătirea pentru control înseamnă trasabilitate, nu cosmetizare.

Livrabil	Descriere
Raport audit/ preaudit	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Constatări clasificate	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.

Plan acțiuni corective	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.

6.15 Raportare incidente și cooperare continuă

Organizația trebuie să aibă procedură de detectare, clasificare, escaladare, notificare și documentare a incidentelor. Raportarea incidentelor este un proces permanent.

Livrabil	Descriere
Playbook incidente	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Registru incidente	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Șabloane notificare	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.
Lecții învățate	Se păstrează în dosarul NIS2 și se actualizează la modificări relevante.

7. Checklist de pregătire pentru notificarea DNSC

Acest checklist poate fi utilizat înainte de transmiterea notificării către DNSC. Pentru fiecare element trebuie păstrată dovada sau justificarea absenței/neaplicabilității.

Element	Ce trebuie verificat	Status
Date de identificare entitate	Denumire, CUI/CIF, sediu, reprezentant legal, date contact	☐
Persoană de contact NIS2	Nume, rol, email, telefon, responsabilitate internă	☐
Sector și subsector	Anexa relevantă, sector, subsector, tip de entitate	☐
Servicii relevante	Serviciile care pot intra în domeniul NIS2 și modul în care sunt furnizate	☐
Dimensiune entitate	Date privind numărul de angajați, cifra de afaceri, bilanț	☐
Sedii și puncte de lucru	Locații relevante pentru furnizarea serviciilor	☐
Sisteme informatice	Aplicații, infrastructuri, rețele, platforme, servicii cloud	☐
Furnizori critici	Furnizori IT, servicii gestionate, cloud, telecom, mentenanță	☐
Justificare încadrare	Argumente pentru entitate esențială, importantă sau neîncadrare	☐
Evaluare perturbare	Dacă este aplicabilă, fișe pe servicii și praguri	☐
Documente suport	Dovezi de dimensiune, servicii, activități, organigramă	☐
Formular notificare	Generat, verificat, semnat de reprezentant legal	☐
Dovadă transmitere	Confirmare platformă/email/depunere fizică	☐
Registru comunicări DNSC	Clarificări, răspunsuri, documente suplimentare	☐

8. Model de dosar NIS2

Un dosar NIS2 bine organizat permite demonstrarea rapidă a trasabilității și reduce riscul de informații dispersate. Recomandarea este ca dosarul să existe atât în format digital controlat, cât și ca index centralizat în platforma CysNis.

Folder recomandat	Conținut
01_Identificare_si_incadrare	Fișe servicii, sector/subsector, dimensiune, justificări de încadrare.
02_Notificare_DNSC	Formular notificare, dovadă transmitere, confirmări, clarificări.
03_Evaluare_perturbare	Fișe de perturbare pe serviciu, praguri, calcule și justificări.
04_Evaluare_risc_ENIRE	Raport risc, scoruri, nivel măsuri, ipoteze și dovezi.
05_Matrice_conformitate	Cerințe, controale, responsabili, dovezi, status, termene.
06_Plan_implementare	Plan aprobat, acțiuni, responsabilități, termene, buget, dependențe.
07_Politici_si_proceduri	Politici, proceduri și instrucțiuni operaționale aprobate.
08_Registre_operationale	Riscuri, active, furnizori, vulnerabilități, incidente, acces, instruiri.
09_Autoevaluare_maturitate	Rapoarte, chestionare, scoring, gap-uri, dovezi.
10_Audit_si_control	Rapoarte audit, constatări, planuri de remediere, dovezi de închidere.
11_Incidente_si_raportari	Cronologii, notificări, decizii, comunicări, lecții învățate.
12_Dovezi_tehnice	Capturi, rapoarte scanare, loguri relevante, rezultate teste backup/restore.

9. RACI extins de responsabilități

RACI: R = responsabil execuție, A = aprobă/asumă, C = consultat, I = informat. Matricea trebuie adaptată fiecărei organizații.

Activitate	Mgmt	Resp. NIS2	IT/Sec	Juridic/Ach.	HR	Consultant	Audit
Decizie inițiere NIS2	A	C	C	C	I	R/C	C
Colectare date identificare	I	R	C	C	C	R	C
Analiză sector/subsector	A	R	C	C	I	R/C	C
Notificare DNSC	A	R	C	C	I	C	C
Evaluare perturbare	A	R	C	C	C	R/C	C
Evaluare nivel risc	A	R	C	C	C	R/C	C
Matrice conformitate	I	R	C	C	I	R	C
Plan implementare	A	R	C	C	C	R	C
Implementare controale tehnice	I	C	R	C	I	C	C
Management furnizori	I	C	C	R	C	C	C
Instruire și conștientizare	I	C	C	C	R	C	I
Raportare incidente	A/I	R	R/C	C	I	C	C
Autoevaluare maturitate	A	R	C	C	C	R/C	C
Audit/preaudit	I	R	C	C	C	C	R/C
Raportare către management	A	R	C	C	C	C	I

10. Documente și registre minime recomandate

Documentația trebuie construită gradual, pe măsură ce controalele sunt implementate. Existența unui document fără aplicare și fără dovezi nu este suficientă.

10.1 Documente pentru inițiere și notificare

- decizie internă de demarare NIS2;
- fișă de identificare și încadrare;
- formular de notificare DNSC și dovada transmiterii;
- evaluarea gradului de perturbare, dacă este aplicabilă;
- raport de evaluare a nivelului de risc;
- registru inițial de riscuri;
- matrice de conformitate;
- plan de implementare aprobat.

10.2 Documente pentru implementare

- politica de securitate a informațiilor și securitate cibernetică;
- metodologia de management al riscului;
- procedura de gestionare și raportare a incidentelor;
- politica de backup și procedura de restaurare;
- plan de continuitate și plan de recuperare în caz de dezastru;
- politica de control acces și autentificare multifactor;
- politica de securitate a furnizorilor și lanțului de aprovizionare;
- procedura de management al vulnerabilităților și patching;
- politica de criptografie și comunicații securizate;
- plan de instruire și conștientizare.

10.3 Registre operaționale recomandate

Registru	Câmpuri minime
Registru riscuri	ID, serviciu, activ, amenințare, vulnerabilitate, impact, probabilitate, nivel, tratament, responsabil, termen, risc rezidual.
Registru active	ID activ, proprietar, criticitate, locație, sistem, date procesate, dependențe, status, măsuri aplicate.
Registru furnizori	Furnizor, serviciu, criticitate, contract, cerințe securitate, SLA, evaluare, incident istoric, deținător.
Registru vulnerabilități	ID, activ, severitate, sursă, CVE, responsabil, termen remediere, status, dovadă.
Registru incidente	ID, dată, categorie, severitate, impact, decizii, notificări, măsuri, lecții învățate.
Registru acces	Conturi privilegiate, proprietar, aprobare, justificare, revizuire, MFA, dezactivare.
Registru instruiri	Curs, dată, participanți, rezultate, absențe, acțiuni corective.
Registru excepții	Cerință, excepție, risc, justificare, aprobare management, termen revizuire.

10.4 Documente pentru audit și control

- registru de incidente și cronologii de răspuns;
- registru de vulnerabilități și dovezi de remediere;
- rapoarte de testare backup/restore;
- rapoarte de instruire și prezență;
- rapoarte de audit intern/preaudit;
- planuri de remediere și dovezi de închidere;
- minute ale ședințelor de management privind riscurile și conformarea.

11. Matrice operațională Art. 21: cerințe, controale, dovezi

Matricea de mai jos nu reproduce exhaustiv textele legale, ci oferă o traducere operațională a principalelor domenii de măsuri în controale și dovezi. Ea trebuie adaptată în funcție de nivelul de risc, sector, mărime, tehnologie și externalizări.

Domeniu măsuri	Controale operaționale	Dovezi recomandate	Responsabil
Politici de analiză a riscurilor și securitatea SI	Metodologie risc; politică securitate; revizuire periodică; aprobare management.	Politică aprobată, registru riscuri, minute management, rapoarte de revizuire.	Mgmt / Resp. NIS2
Gestionarea incidentelor	Procedură incident; clasificare; triere; escaladare; notificare; post-incident review.	Registru incidente, tichete, loguri, cronologii, notificări, lecții învățate.	IT/Sec / Resp. NIS2
Continuitate, backup și recuperare	BIA; RTO/RPO; backup regulat; backup offline/ immutabil; teste restore; DRP/BCP.	BIA, plan BCP/DRP, rapoarte backup, teste restore, procese-verbale exerciții.	IT / Operațional
Securitatea lanțului de aprovizionare	Clasificare furnizori; cerințe contractuale; due diligence; monitorizare; clauze de incident.	Registru furnizori, chestionare, contracte, SLA, rapoarte evaluare, notificări furnizori.	Achiziții / Juridic / IT
Securitate în achiziția, dezvoltarea și întreținerea sistemelor	Security by design; change management; testare; segregare medii; management release.	Cerințe proiect, aprobări change, teste securitate, code review, scanări, rapoarte release.	IT / Dezvoltare
Evaluarea eficacității măsurilor	KPI/KRI; audit intern; teste tehnice; exerciții; revizuire management.	Rapoarte audit, scanări, rezultate exerciții, dashboard, decizii management.	Audit / Resp. NIS2
Igienă cibernetică și instruire	Program awareness; simulări phishing; reguli parole/MFA; patching; utilizare sigură.	Plan instruire, liste participanți, rezultate teste, materiale, rapoarte phishing.	HR / IT/Sec
Criptografie și criptare	Politică criptografie; TLS; criptare date la rest/tranzit; management chei.	Politică, configurații, certificate, inventar chei, dovezi criptare.	IT/Sec
Resurse umane, control acces și active	Onboarding/ offboarding; least privilege; revizuire acces; inventar active.	Procese HR, cereri acces, revizuiri, registru active, listă conturi privilegiate.	HR / IT / Deținători
MFA și comunicații	MFA pentru acces privilegiat/	Configurații MFA, rapoarte	IT/Sec

securizate	remote; VPN; email security; comunicare criptată.	utilizatori, politici VPN, loguri autentificare.	

12. Roadmap de implementare 30/60/90 zile și calendar anual

Roadmap-ul trebuie adaptat în funcție de decizia DNSC, nivelul de risc, resurse și gradul de maturitate. Varianta de mai jos este un punct de plecare practic.

Perioadă	Prioritate	Livrabile principale
0-30 zile	Guvernanță și identificare	Decizie internă, echipă, colectare date, fișă servicii, utilizare mecanisme DNSC, notificare, dosar NIS2.
31-60 zile	Risc și planificare	Evaluare perturbare, evaluare risc, matrice conformitate, registru riscuri, plan implementare aprobat.
61-90 zile	Controale prioritare	Incident management, backup/restore, control acces/MFA, inventar active, furnizori critici, instruire inițială.
3-6 luni	Operaționalizare	Politici/proceduri aprobate, patching, vulnerabilități, BCP/DRP, monitorizare, registru dovezi, exerciții.
6-12 luni	Maturizare și audit	Autoevaluare maturitate, audit/preaudit, plan remediere, testare furnizori, simulare incident, raport management.

Calendar anual minim recomandat

Frecvență	Activitate
Lunar	Raport progres NIS2, riscuri deschise, incidente, vulnerabilități, acțiuni întârziate.
Trimestrial	Revizuire management, status plan, furnizori critici, acces privilegiate, KPI/KRI.
Semestrial	Exercițiu incident, test restaurare, revizuire BCP/DRP, refresh awareness.
Anual	Autoevaluare maturitate, audit intern/ preaudit, revizuire politici, revizuire risc, plan buget.
La modificări majore	Reevaluare încadrare/ risc pentru servicii noi, M&A, externalizări, incidente majore, schimbări infrastructură.

13. Managementul riscurilor: registru, tratament, risc rezidual

Managementul riscurilor trebuie să fie legat direct de serviciile NIS2, nu doar de active IT izolate. Un risc relevant trebuie să descrie serviciul afectat, scenariul de amenințare, vulnerabilitatea, impactul, probabilitatea, controlul existent, măsura de tratament și riscul rezidual.

Câmp registru	Descriere
ID risc	Cod unic: R-NIS2-001 etc.
Serviciu afectat	Serviciul relevant NIS2 sau procesul de suport.
Activ / sistem	Aplicație, rețea, server, furnizor, proces, persoană.
Amenințare	Ex. ransomware, indisponibilitate cloud, acces neautorizat, eroare umană.
Vulnerabilitate	Ex. lipsă MFA, patching întârziat, contract fără clauze de incident.
Impact	Operațional, financiar, legal, reputațional, societal.
Probabilitate	Scor sau calificativ justificat.
Nivel risc inerent	Înainte de tratament.
Controale existente	Măsuri deja implementate.

Tratament	Reducere, evitare, transfer, acceptare.
Responsabil	Deținător de risc și deținător de acțiune.
Termen	Data țintă pentru acțiune.
Risc rezidual	Nivel după măsuri; necesită aprobare management dacă rămâne semnificativ.

Regulă de maturitate

Un registru de riscuri este util doar dacă produce decizii. Fiecare risc semnificativ trebuie să aibă un responsabil, tratament, termen și dovadă de urmărire.

14. Playbook pentru incidente și raportare

Raportarea incidentelor este un proces permanent. Organizația trebuie să poată detecta, clasifica, escalada, decide, documenta și raporta incidentul conform obligațiilor aplicabile.

Fază	Ce se face	Dovezi
1. Detectare	Alertă tehnică, raportare utilizator, furnizor, monitorizare, media, autoritate.	Tichet, loguri, capturi, sursă alertă.
2. Triage	Se confirmă dacă evenimentul este incident, severitatea și serviciile afectate.	Fișă triage, decizie inițială.
3. Escaladare	Se informează responsabilul NIS2, IT/Sec, management, juridic și comunicare, după caz.	Jurnal decizii, listă notificări interne.
4. Limitare	Se aplică măsuri de izolare pentru reducerea impactului.	Comenzi, loguri, tichete, aprobări de urgență.
5. Analiză impact	Se evaluează impactul asupra serviciului, datelor, utilizatorilor, furnizorilor și obligațiilor.	Raport impact, cronologie, dovezi tehnice.
6. Notificare	Se urmează procedura de notificare DNSC și, după caz, alte autorități/terți.	Formulare, confirmări, emailuri, registru raportare.
7. Eradicare și recuperare	Se elimină cauza, se restaurează, se verifică integritatea și se monitorizează.	Rapoarte restore, IOC, scanări, teste.
8. Lecții învățate	Se actualizează controalele, riscurile, procedurile și instruirea.	Post-incident review, plan de acțiuni, dovezi închidere.

Model minim de registru incidente

Câmp	Exemplu / cerință
ID incident	INC-YYYY-001
Data și ora detectării	Timestamp și fus orar
Sursă detectare	SIEM, utilizator, furnizor, EDR, altă autoritate
Servicii afectate	Servicii NIS2 și sisteme suport
Categorie	Confidențialitate / integritate / disponibilitate / mixt
Severitate	Scăzută / medie / ridicată / critică
Impact estimat	Utilizatori, durată, date, operațiuni, furnizori
Decizii	Cine a decis, ce a decis, când
Notificări	DNSC, ANSPDCP, clienți, furnizori, sectorial

Măsuri	Limitare, eradicare, recuperare, comunicare
Lecții învățate	Acțiuni preventive și termene

15. Managementul furnizorilor și lanțului de aprovizionare

Securitatea lanțului de aprovizionare este una dintre zonele în care conformarea formală eșuează frecvent. Organizația trebuie să identifice furnizorii critici, să includă cerințe contractuale și să monitorizeze riscurile pe durata relației.

Etapă	Cerință practică
Identificare	Lista furnizorilor care susțin servicii NIS2: cloud, telecom, MSP, software, mentenanță, procesatori date.
Clasificare criticitate	Critic / important / suport, pe baza impactului asupra serviciului și datelor.
Due diligence	Chestionar securitate, certificări, controale, istoricul incidentelor, localizarea datelor, subcontractori.
Contractare	Clauze de securitate, incident reporting, audit, SLA, confidențialitate, continuitate, exit plan.
Monitorizare	Revizuiri periodice, rapoarte, incidente, schimbări majore, teste sau audituri.
Ieșire / transfer	Plan de exit, backup date, ștergere/returnare date, revocare acces, continuitate.

Clauze contractuale recomandate pentru furnizori critici

- obligații minime de securitate și confidențialitate;
- notificare rapidă a incidentelor care pot afecta serviciile organizației;
- drept de audit sau drept de solicitare de dovezi/ rapoarte;
- cerințe privind subcontractorii și localizarea datelor;
- SLA pentru disponibilitate, suport și recuperare;
- cerințe de backup, continuitate și exit;
- obligații privind patching, vulnerabilități și schimbări majore;
- păstrarea și furnizarea logurilor relevante, unde este aplicabil.

16. Audit, autoevaluare și pregătire pentru control

Auditul și autoevaluarea trebuie să confirme existența și eficacitatea controalelor. Pregătirea pentru control nu înseamnă cosmetizarea documentelor, ci capacitatea de a demonstra rapid ce s-a decis, ce s-a implementat, cine răspunde și ce dovezi există.

Fază audit	Activități
Planificare	Mandat, domeniu, criterii, perioadă, echipă, lista documentelor necesare.
Analiză documentară	Politici, proceduri, registre, rapoarte, decizii, dovezi tehnice.
Interviuri	Management, IT, operațional, juridic, HR, achiziții, responsabili servicii.
Testare / verificare	Eșantionare controale: acces, backup, patching, incidente, furnizori, instruire.
Constatări	Clasificare: critică, majoră, minoră, observație, oportunitate de îmbunătățire.
Raportare	Raport audit/preaudit, concluzii, neconformități, recomandări, plan remediere.
Urmărire	Dovezi de închidere, verificare eficacitate, actualizare registru riscuri.

Pachet minim pentru audit/preaudit

- decizie internă și RACI;
- fișă încadrare și notificare DNSC;
- evaluare perturbare și evaluare risc;
- matrice conformitate și plan implementare;
- politici și proceduri aprobate;
- registre operaționale actualizate;
- dovezi tehnice și rapoarte de testare;
- rapoarte de instruire;
- rapoarte management;
- planuri de remediere și dovezi închidere.

17. Ce trebuie să știe conducerea

Conducerea organizației are un rol direct în aprobarea măsurilor, supravegherea implementării și înțelegerea riscurilor cibernetice. NIS2 nu transferă responsabilitatea integrală către IT, consultant sau responsabilul extern.

- managementul trebuie să aprobe direcția, resursele și prioritățile;
- riscurile cibernetice trebuie tratate ca riscuri operaționale și de continuitate;
- raportarea periodică către conducere trebuie să includă progres, blocaje, riscuri reziduale și neconformități;
- externalizarea consultanței sau a rolului operațional nu elimină obligația de supraveghere a managementului;
- dovezile de decizie, aprobare și revizuire trebuie păstrate în dosarul NIS2.

Întrebare pentru conducere

Putem demonstra, pe baza unor dovezi, că știm ce servicii NIS2 furnizăm, ce nivel de risc avem, ce măsuri aplicăm și ce acțiuni sunt încă deschise?

Raport lunar recomandat către conducere

Secțiune raport	Conținut minim
Status general	verde/galben/roșu, progres față de plan, principalele blocaje.
Riscuri principale	top 5 riscuri, risc rezidual, decizii necesare.
Incidente și vulnerabilități	incidente, vulnerabilități critice, acțiuni întârziate.
Furnizori critici	evaluări, probleme contractuale, incidente furnizori.
Dovezi și audit	documente aprobate, dovezi lipsă, constatări audit/preaudit.
Decizii solicitate	buget, resurse, acceptări de risc, priorități.

18. Greșeli frecvente și cum se evită

Greșeală	Impact	Cum se evită
Se pornește de la documente, nu de la încadrare	Documentele pot fi irelevante dacă organizația nu știe exact ce obligații i se aplică.	Începeți cu identificarea serviciilor, sectorului și notificarea fundamentată.
Se folosește doar codul	Codul CAEN poate ajuta, dar	Documentați serviciile reale și

CAEN	serviciul furnizat și rolul real sunt determinante.	corespondentul lor în anexele aplicabile.
Notificarea DNSC este tratată ca formular simplu	Notificarea trebuie susținută de analiză, justificări și dovezi.	Păstrați dosar de notificare și jurnal de ipoteze.
Checklistul este folosit ca dovadă de conformitate	Checklistul este instrument de verificare, nu dovadă în sine.	Atașați dovezi pentru fiecare răspuns „conform”.
ISO 27001 este considerat automat suficient	Certificarea poate ajuta, dar cerințele NIS2/DNSC trebuie documentate separat.	Faceți mapare între certificare, controale, cerințe și dovezi.
Responsabilitatea este lăsată exclusiv la IT	NIS2 este o obligație de guvernanță, risc și management.	Includeți managementul în aprobare, raportare și acceptare de risc.
Furnizorii sunt ignorați	Lanțul de aprovizionare este parte explicită a măsurilor de securitate.	Clasificați furnizorii critici și actualizați contractele.
Nu se păstrează dovezi	Fără dovezi, implementarea nu poate fi demonstrată în audit sau control.	Mențineți registru dovezi și dosar NIS2 controlat.

19. Cum ajută platforma CysNis

CysNis este utilă atunci când este folosită ca platformă de organizare a conformării, nu ca substitut al analizei. Platforma poate centraliza fluxul de lucru, dovezile, documentele și statusul implementării.

Consultați prezentarea platformei **CyNis**: https://cysnis.eu/prezentare-platforma

Componentă	Valoare practică
Identificare și încadrare	Structurarea datelor privind sectorul, serviciile, justificările și statusul încadrării.
Notificare și dosar DNSC	Organizarea formularului, dovezilor, comunicărilor și documentelor suport.
Evaluare perturbare/risc	Centralizarea ipotezelor, scorurilor, justificărilor și nivelului de măsuri aplicabil.
Matrice conformitate	Legarea cerințelor de controale, documente, responsabilități și dovezi.
Plan implementare	Urmărirea acțiunilor, termenelor, responsabililor și statusului.
Documente și registre	Generarea politicilor, procedurilor, registrelor sub formă de draft personalizat sau analizarea și remedierea celor existente.
Audit și raportare	Pregătirea pachetului de audit, urmărirea constatărilor și planurilor de remediere.
Incidente	Suport pentru evidența incidentelor, cronologii, decizii și lecții învățate.
Management	Cont special de monitorizare și raportare a nivelului de implementare.

Poziționare corectă

CysNis nu „înlocuiește” DNSC și nu decide încadrarea. CysNis ajută organizația să lucreze structurat, să păstreze dovezi și să urmărească progresul în logica reglementată.

20. Contractarea unui consultant Prodefence

Contractarea unui consultant Prodefence este recomandată în special din etapa de pornire, când organizația trebuie să evite erorile de încadrare, notificare, evaluare și planificare.

Experții echipei Prodefence sunt auditori NIS2 acreditați de Directoratul Național de Securitate Cibernetică, auditori de certificare ISO/ IEC 27001, auditori IT, responsabili implementare NIS2, auditori tehnici de securitate cibernetică(Pentesting).

20.1 Când este recomandat consultantul

- încadrarea este incertă sau organizația are activități în mai multe sectoare;
- există servicii critice, furnizori importanți sau dependențe tehnologice complexe;
- organizația nu are intern competențe NIS2 suficiente;
- se pregătește notificarea către DNSC;
- se dorește un plan de implementare realist, pe risc și pe dovezi;
- organizația se pregătește pentru audit, preaudit sau control.

20.2 Ce poate livra consultantul Prodefence

- analiză de încadrare și justificare documentată;
- verificarea datelor pentru notificare DNSC;
- evaluare perturbare și evaluare risc;
- gap analysis și autoevaluare maturitate;
- matrice de conformitate;
- plan de implementare și plan de remediere;
- pachet documentar adaptat organizației;
- pregătire pentru audit și suport pentru management.

20.3 Livrabile contractuale

Livrabil	Descriere	Moment
Raport de încadrare	Analiză sector/subsector, servicii, dimensiune și justificare.	Inițiere
Lista documentelor de evaluare	Listă documente și date necesare pentru evaluare.	Inițiere
Raport GAP	Diferențe între cerințe și situația curentă.	După interviuri
Matrice conformitate	Cerințe, controale, dovezi, status.	După evaluare
Plan implementare	Acțiuni, responsabili, termene, priorități.	După risc
Pachet documentar	Politici, proceduri, registre, șabloane.	Implementare
Raport preaudit	Constatări, risc, recomandări, plan remediere.	Validare

21. Responsabil NIS2 extern prin Prodefence

Pentru organizațiile care nu au intern un CISO, un responsabil de securitate cibernetică sau o funcție dedicată de conformitate NIS2, contractarea unui responsabil NIS2 extern prin Prodefence poate asigura continuitatea procesului.

Detalii: https://www.prodefence.ro/responsabil-nis2-externalizat/

21.1 Când este util

- responsabilul IT nu are timp sau competențe suficiente pentru coordonarea NIS2;
- managementul dorește raportare periodică și disciplină de implementare;
- există multe departamente implicate și este nevoie de coordonare;
- trebuie urmărite acțiuni, registre, dovezi, incidente și audituri;
- organizația dorește pregătire continuă pentru verificări și control.

21.2 Ce face responsabilul NIS2 extern

- coordonează calendarul și planul NIS2;
- menține matricea de conformitate și registrele relevante;
- urmărește acțiunile deschise și dovezile de închidere;
- pregătește rapoarte periodice pentru management;
- sprijină pregătirea auditului și a controalelor;
- coordonează documentar procesul de raportare a incidentelor;
- asigură legătura operațională între management, IT, juridic, achiziții și consultant.

Limită importantă
Responsabilul NIS2 extern sprijină și coordonează. El nu elimină responsabilitatea de guvernanță a conducerii și nu înlocuiește deciziile autorității competente.

22. Mini-studii de caz

22.1 Organizație de producție cu furnizori digitali critici

Element	Descriere
Situația inițială	Lipsă fișă de încadrare, documente dispersate, furnizori critici neevaluați, fără registru de riscuri.
Acțiunea 1	Se colectează serviciile, sistemele și furnizorii relevanți. Se verifică sectorul, subsectorul și rolul organizației.
Acțiunea 2	Se folosește mecanismul DNSC pentru identificare și notificare. Se pregătesc justificări și dovezi.
Acțiunea 3	Se evaluează perturbarea serviciilor și nivelul de risc. Se stabilește nivelul de măsuri aplicabil.
Acțiunea 4	Se construiesc matricea de conformitate, registrul de riscuri și planul de implementare.
Acțiunea 5	Se implementează controale privind accesul, backup, incidente, furnizori, patching, instruire și continuitate.
Rezultat	Organizația are dosar NIS2 structurat, plan de implementare urmărit, dovezi centralizate și pregătire pentru audit/preaudit.

22.2 Spital sau furnizor de servicii medicale

Element	Descriere
Situația inițială	Servicii medicale dependente de HIS, PACS, laborator, rețea, furnizori IT și echipamente conectate.

Riscuri tipice	Ransomware, indisponibilitate sisteme clinice, acces neautorizat la date, furnizori de mentenanță fără clauze clare.
Priorități	Continuitate, backup testat, segmentare, acces privilegii, procedură incident, furnizori critici, exercițiu de criză.
Dovezi	BIA, teste restore, registru active medicale conectate, proceduri incidente, instruire personal, rapoarte de vulnerabilități.

22.3 Furnizor digital / serviciu cloud sau SaaS

Element	Descriere
Situația inițială	Servicii digitale furnizate clienților, infrastructură cloud, devops, subcontractori, suport 24/7.
Riscuri tipice	Compromitere identități, indisponibilitate serviciu, vulnerabilități aplicație, atac DDoS, scurgere date.
Priorități	MFA, CI/CD securizat, logging, vulnerability management, incident response, SLA, backup, segregare clienți.
Dovezi	Rapoarte scanare, proceduri change/release, loguri, contracte furnizori cloud, teste DR, rapoarte incidente.

23. Checklist final de autoverificare

Întrebare	Status
Știm exact sectorul, subsectorul și tipul de entitate aplicabil?	☐
Am documentat serviciile relevante și sistemele care le susțin?	☐
Am utilizat mecanismul DNSC aplicabil pentru identificare/notificare?	☐
Avem formularul de notificare și dovada transmiterii?	☐
Am păstrat comunicările și clarificările cu DNSC?	☐
Am evaluat perturbarea serviciilor relevante, unde este aplicabil?	☐
Am determinat nivelul de risc și nivelul de măsuri aplicabil?	☐
Avem matrice de conformitate corelată cu cerințele și dovezile?	☐
Avem plan de implementare aprobat de conducere?	☐
Avem registre pentru riscuri, active, furnizori, vulnerabilități și incidente?	☐
Putem demonstra controalele prin dovezi, nu doar prin declarații?	☐
Avem procedură de raportare a incidentelor și responsabil desemnat?	☐
Avem plan de autoevaluare, audit și remediere?	☐
Managementul primește periodic raportări privind riscurile și progresul?	☐

24. Modele și anexe operaționale

Anexele de mai jos pot fi copiate și adaptate în documentele interne ale organizației. Ele sunt modele operaționale minimale, nu substituie analiza individuală.

24.1 Model: Decizie internă de demarare NIS2

Câmp	Conținut recomandat
Titlu	Decizie internă privind inițierea procesului de conformare NIS2.
Temei	Directiva NIS2, OUG 155/2024, Legea 124/2025 și ordinele DNSC aplicabile.
Scop	Stabilirea echipei, responsabilităților și calendarului pentru identificare, notificare și conformare.
Factor decizional management	Nume, funcție, responsabilitate de aprobare și escaladare.
Responsabil NIS2	Nume/rol intern sau extern, atribuții operaționale.
Echipă	IT, juridic, achiziții, HR, operațional, audit intern, comunicare.
Livrabile	Fișă încadrare, notificare, evaluare risc, matrice, plan implementare, registre, audit.
Raportare	Lunar către conducere sau ori de câte ori apar schimbări/incident.

24.2 Model: Fișă serviciu relevant NIS2

Câmp	Descriere
Denumire serviciu	Numele serviciului furnizat.
Sector/subsector	Încadrarea operațională în anexele aplicabile.
Beneficiari	Clienți, cetățeni, pacienți, utilizatori, parteneri.
Sisteme suport	Aplicații, infrastructură, cloud, rețea, OT/ICS.
Date procesate	Categorii de date și criticitate.
Furnizori dependenți	Furnizori fără de care serviciul este afectat.
Toleranță indisponibilitate	RTO/RPO sau praguri interne.
Impact perturbare	Operațional, societal, financiar, legal.
Deținător serviciu	Responsabil business/operațional.

24.3 Model: Raport lunar NIS2 către management

Secțiune	Întrebări de răspuns
Status general	Suntem în termen? Ce etape sunt finalizate?
Riscuri majore	Care sunt riscurile critice și deciziile necesare?
Acțiuni întârziate	Ce acțiuni sunt întârziate, cine este responsabil, ce blocaj există?
Incidente	Au existat incidente, vulnerabilități critice sau alerte relevante?
Furnizori	Ce furnizori critici nu sunt evaluați sau nu au clauze adecvate?
Dovezi lipsă	Ce controale sunt declarate, dar nedemonstrate?
Decizii solicitate	Buget, personal, acceptări de risc, prioritizare.

24.4 Model: Lista documentelor pentru proiect NIS2

- organigramă și responsabilități;
- descriere servicii și procese operaționale;
- liste aplicații, servere, echipamente, servicii cloud;
- contracte cu furnizori IT/critici;

- politici și proceduri de securitate existente;
- rapoarte de audit, pentest, scanare vulnerabilități;
- registre incidente, tichete, proceduri suport;
- planuri de backup, continuitate, recuperare;
- rapoarte instruire și conștientizare;
- decizii sau comunicări anterioare cu autorități.

24.5 Model: Criterii interne de clasificare a constatărilor

Nivel	Descriere	Exemplu
Critic	Deficiență cu impact major imediat asupra serviciilor, raportării sau securității.	Lipsă backup funcțional pentru serviciu critic; compromitere activă.
Major	Neconformitate relevantă care afectează conformarea sau riscul.	Lipsă procedură incident; lipsă MFA pentru acces privilegiat.
Minor	Deficiență documentară sau operațională cu impact limitat.	Politică nerevizuită; registru incomplet parțial.
Observație	Aspect de îmbunătățit fără neconformitate clară.	Raport management poate fi mai granular.

25. Referințe normative și bibliografie

- Uniunea Europeană. Directiva (UE) 2022/2555 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune (NIS2).
- Guvernul României. OUG nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil.
- Parlamentul României. Legea nr. 124/2025 pentru aprobarea OUG nr. 155/2024, cu modificări și completări.
- Directoratul Național de Securitate Cibernetică. Ordinul directorului DNSC nr. 1/2025 privind procesul de notificare în vederea înregistrării și metoda de transmitere a informațiilor.
- Directoratul Național de Securitate Cibernetică. Ordinul directorului DNSC nr. 2/2025 privind criteriile și pragurile de determinare a gradului de perturbare și metodologia de evaluare a nivelului de risc.
- Directoratul Național de Securitate Cibernetică. Ordinul directorului DNSC nr. 3/2025 privind supravegherea, verificarea și controlul respectării OUG nr. 155/2024.
- ENISA. Ghiduri și recomandări privind NIS2, securitatea lanțului de aprovizionare, managementul incidentelor și bune practici de securitate cibernetică.
- ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 și ISO 22301, utilizate ca bune practici pentru organizarea controalelor și managementului riscurilor.

NIS2 nu începe cu checklistul și nu începe cu documentele. NIS2 începe cu identificarea corectă, notificarea fundamentată, evaluarea riscului și stabilirea măsurilor aplicabile.

Organizațiile care respectă fluxul DNSC pot demonstra nu doar că au documente, ci că au un proces funcțional de securitate cibernetică: guvernanță, risc, controale, dovezi, audit și raportare continuă.

Recomandare practică

Pentru o implementare ghidată, contractați un consultant Prodefence pentru etapele de identificare, notificare, evaluare și implementare. Pentru coordonare permanentă, contractați un responsabil NIS2 extern prin Prodefence.

Resurse utile

Ghid vizual - NIS2 România – Ghid complet de la înțelegere la implementare

Curs introductiv - Directiva privind Securizarea Rețelelor și a Informațiilor (NIS2)

Informații **Prodefence**	Informații **CysNis**
Pagina web: www.prodefence.ro Email: contact@prodefence.ro Telefon: +40763204739	Platformă: www.cysnis.eu Despre CysNis: www.cysnis.eu/despre Prezentare: www.cysnis.eu/prezentare-platformă