GMB since 1991 COMPUTERS

CYMAROP
www.cymarop.ro

CENTRUL OPERAȚIONAL DE SECURITATE CIBERNETICĂ GMB COMPUTERS

Implementarea Directivei NIS2 în România

Aspecte legale și tehnice referitoare la înrolarea, identificarea, clasificarea și validarea entităților, evaluări de risc de securitate cibernetică, autoevaluări de maturitate la nivelul entităților înrolate

AUDITOR NIS
ATESTAT DE SECURITATE CIBERNETICĂ
LEGEA nr 362/2018

Rezumat: Legea nr. 124/2025 consolidează transpunerea Directivei NIS2 în România, aducând clarificări și măsuri stricte pentru protecția rețelelor și sistemelor informatice. Actul normativ armonizează cerințele cu legislația existentă, protejează confidențialitatea raportărilor către Directoratul Național de Securitate Cibernetică („DNSC") și responsabilizează managementul prin obligația de formare și desemnarea unui CISO. Prin proiectele de ordine subsecvente Legii, DNSC facilitează înrolarea, evaluarea riscurilor și autoevaluarea maturității entităților esențiale și importante odată cu iminenta operaționalizare a unei platforme web dedicată. Conformarea reduce riscul de atacuri și crește încrederea partenerilor, însă implică investiții în tehnologie, personal și audituri. Neconformarea atrage amenzi severe, răspundere personală și pierderi reputaționale, fiind vitală acțiunea rapidă pentru implementarea măsurilor cerute.

Cuvinte cheie: NIS2, OUG 155/2024, Legea 124/2025, DNSC, securitate cibernetică, entitate esențială, entitate importantă, conformare, audit de securitate, risc cibernetic, autoevaluare maturitate, incident semnificativ, CISO, cooperare transfrontalieră, protecția datelor, responsabilitate management, reziliență operațională, amenzi, reputație, infrastructură critică.

Introducere

În ultimele două decenii, am asistat la o creștere exponențială a digitalizării. Tot mai multe servicii vitale – energie, apă, sănătate, transport, comunicații, dar și administrație publică – au migrat în spațiul virtual, creând o interdependență digitală fără precedent. „Comisia (Europeană n.r.) este hotărâtă să transforme această perioadă în „deceniul digital" al Europei. Uniunea trebuie să își consolideze suveranitatea digitală și să-și stabilească propriile standarde în loc să le urmeze pe ale altora, cu un accent clar pe date, tehnologie și infrastructură".
Însă, odată cu aceste avantaje, au crescut și vulnerabilitățile. **Atacurile cibernetice** au devenit instrumente strategice, la îndemâna actorilor statali sau non statali, atât în conflictele geopolitice cât și în domeniul criminalității organizate. De la atacurile cibernetice pe scară largă asupra infrastructurii energetice ucrainene, la incidente precum ransomware-ul care a afectat spitalele românești în 2024, luând două exemple orchestrate în scopuri diferite, se poate confirma încă o dată că securitatea cibernetică nu mai este doar o chestiune tehnică, ci una de securitate națională și europeană.

În acest context, Uniunea Europeană a adoptat Directiva (UE) 2022/2555 (NIS2), o reglementare mai strictă și mai detaliată decât predecesoarea sa, Directiva NIS din 2016. România, la rândul ei, a transpus aceste prevederi prin OUG nr. 155/2024, consolidată ulterior de Legea nr. 124/2025. Această legislație reprezintă unul dintre cele mai solide instrumente legislative în materie de securitate cibernetică din Uniune.
În cele ce urmează, vom explora noutățile aduse de Legea nr. 124/2025, implicațiile acesteia asupra mediului public și privat, și riscurile, inclusiv pecuniare, ale neconformării.

Modificările și clarificările aduse de Legea nr. 124/2025 la OUG nr. 155/2024

Adoptarea Legii nr. 124/2025 („Legea") nu s-a limitat la aprobarea OUG nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil, ci a adus modificări importante, menite să facă legea mai clară, mai riguroasă și mai aplicabilă în practică.
În primul rând, Legea precizează explicit că OUG nr. 155/2024 nu se aplică în contradicție cu alte acte normative esențiale, precum GDPR, Legea nr. 506/2004 privind protecția vieții private în comunicațiile electronice, Codul Penal, sau Regulamentul DORA privind reziliența operațională digitală în sectorul financiar. Acest lucru este vital, pentru că aduce asigurări că operatorii economici nu sunt prinși între obligații contradictorii.

Totodată, Legea aduce clarificări importante privind regimul confidențialității informațiilor transmise către Directoratul Național de Securitate Cibernetică („DNSC"). Astfel, datele raportate, inclusiv rapoartele privind incidentele cibernetice, nu sunt considerate informații de interes public, conform Legii nr. 544/2001. Aceasta reprezintă o garanție crucială pentru companii, întrucât oferă protecție împotriva dezvăluirii publice a unor vulnerabilități sau detalii sensibile despre infrastructura lor IT sau businessul în derulare.

Un punct major al noii Legi este legat de responsabilitatea și responsabilizarea managementului. Membrii organelor de conducere nu mai pot rămâne în postura de „simpli beneficiari" ai serviciilor IT. Legea îi obligă să urmeze

cursuri de formare acreditate, să înțeleagă riscurile cibernetice și să asigure resursele necesare pentru securizarea rețelelor. În plus, aceștia trebuie să desemneze persoane responsabile (ex. CISO) care să implementeze și să monitorizeze măsurile de securitate la nivelul entităților. Aceasta reprezintă o abordare similară conceptului de accountability consacrat în legislația GDPR. Totodată, se clarifică nevoia ca entitățile esențiale și importante să asigure un nivel suficient de cunoștințe și competențe prin formarea profesională, în mod regulat, a întregului personal.

Legea aduce clarificări suplimentare și în ceea ce privește definiția incidentelor semnificative, sau când impactul unui incident este considerat semnificativ, stabilind criterii precise referitoare la afectarea disponibilității, autenticității, integrității sau confidențialității datelor, impactul asupra serviciilor esențiale, efectele financiare sau reputaționale semnificative.
Această nevoie de claritate este esențială pentru entități, așa cum sunt ele definite de legiuitor, întrucât le ajută să înțeleagă când și ce trebuie raportat către DNSC, evitând atât raportările excesive, cât și riscul de a omite notificări obligatorii.

În plus, Legea întărește obligațiile de cooperare transfrontalieră. România fiind obligată să participe activ la schimburile de informații la nivel european, inclusiv cu ENISA și cu alte state membre, mai ales în cazul incidentelor cibernetice cu impact transfrontalier. Această prevedere reflectă realitatea amenințărilor hibride, în care un atac cibernetic lansat asupra unei țări poate afecta simultan infrastructuri cibernetice critice ale altor state.
Pe plan sancționator, Legea nr. 124/2025 menține nivelul ridicat al amenzilor, dar adaugă precizări:
– procentul se aplică cifrei de afaceri globale, nu doar celei realizate în România,
– se consolidează posibilitatea răspunderii personale a managementului pentru neimplementarea măsurilor de securitate.

Acest mix de sancțiuni financiare și răspundere personală transformă Legea nr. 124/2025 într-un instrument extrem de coercitiv, menit să asigure seriozitate maximă în aplicarea normelor.
Procesul de notificare și instrumentele digitale puse la dispoziție entităților de către DNSC, prin intermediul proiectelor de acte normative subsecvente legii
DNSC, pentru a realiza implementarea prevederilor art. 18 alin. (9) din Ordonanța de urgență a Guvernului nr. 155/2024, urmează să adopte *„Ordinul pentru aprobarea cerințelor privind procesul de notificare în vederea înregistrării și metoda de transmitere a informațiilor”*, aflat în etapa de proiect în Transparenta decizionala, pe site-ul directoratului, www.dnsc.ro.

Un aspect inovator introdus odată cu NIS2 și detaliat în legislația națională este digitalizarea procesului de conformare, DNSC punând la dispoziție atât un instrument digital de evaluare și generare a datelor de notificare, cat și o platformă de înrolare, informare și cooperare. Platforma se utilizează pentru facilitarea proceselor de interacțiune cu entitățile și a păstrării evidenței acestora.

În situația în care platforma este indisponibilă, entitățile vor utiliza instrumentul în procesul de identificare în vederea înscrierii în Registrul entităților, prin generarea formularului de notificare.

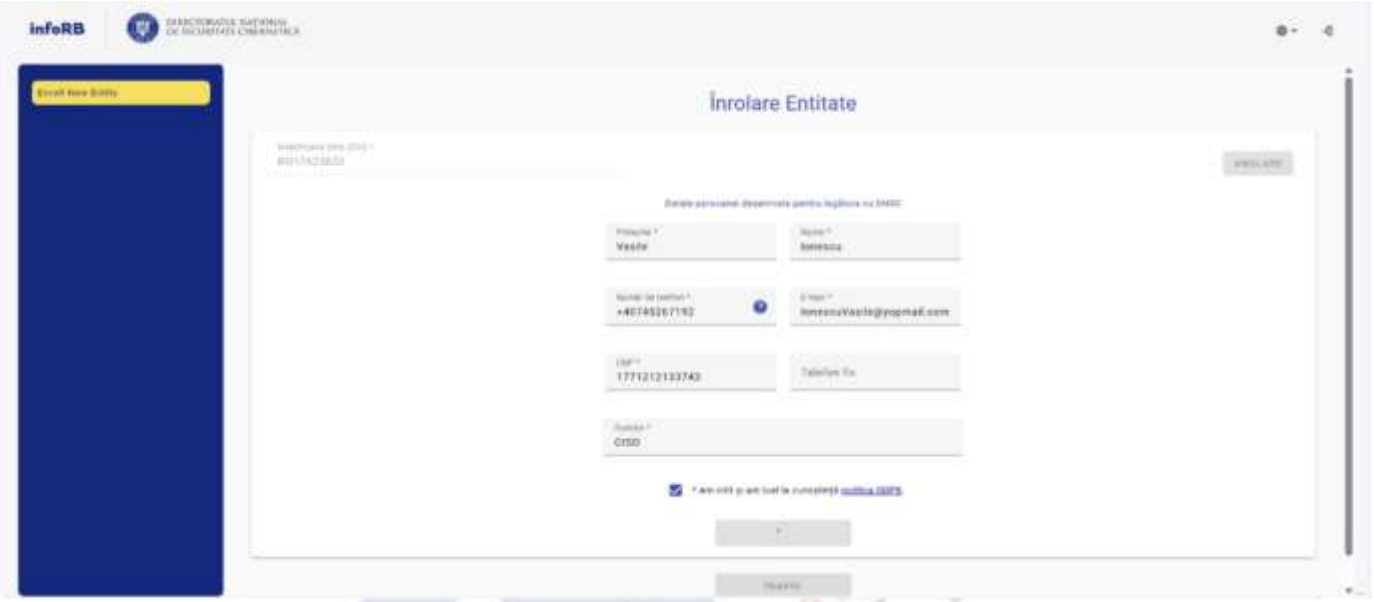
Ghidurile de utilizare, atât a instrumentului, cât și a platformei, sunt incluse în cele două mecanisme specifice și furnizează instrucțiuni despre modalitățile de lucru cu acestea. Legea și ordinele subsecvente reglementează în detaliu pașii pe care entitățile trebuie să-i urmeze, de la colectarea datelor interne până la transmiterea notificării semnate electronic. Totodată, DNSC poate solicita clarificări sau documente suplimentare pentru a stabili corect încadrarea entității drept esențială sau importantă.

Pentru clarificarea timpurie a modalității exacte de lucru cu platforma de înrolare, ce va fi disponibilă, conform proiectului de act normativ, la adresa web platformanis2.ro, vă propunem o parcurgere succintă a capabilităților acesteia.

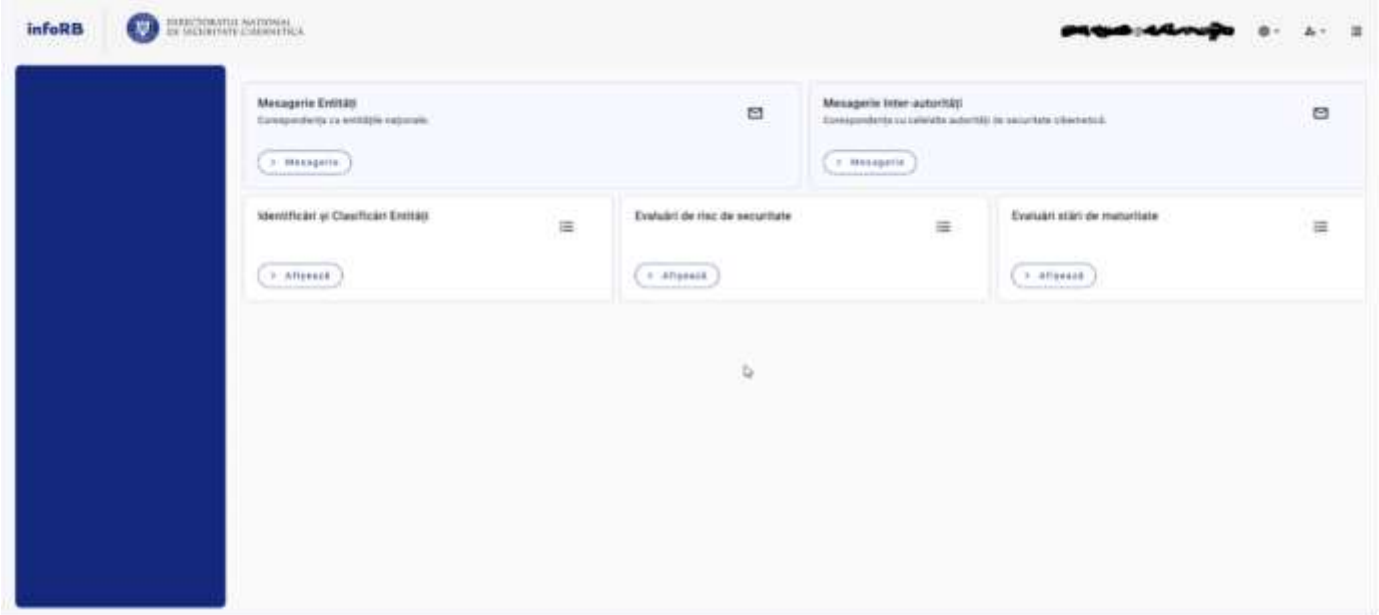
Platforma a fost dezvoltată în mod profesionist de către experții DNSC în cadrul unui proiect cofinanțat de

Comisia Europeană prin European Cybersecurity Competence Centre and Network (ECCC). Informațiile referitoare la evoluția proiectului sunt postate pe pagina internet a instituției și au fost prezentate detaliat în cadrul unor webinare, ocazie cu care s-au făcut demonstrații tehnice practice ale funcționalităților platformei.
În cele ce urmează, vom încerca să descriem acest proces, ce va fi realizat prin utilizarea platformei care urmează a fi pusă la dispoziție online de DNSC.

Astfel, primul pas este cel de înrolare al entității prin furnizarea datelor persoanei desemnate pentru relația cu DNSC. În cadrul imaginilor, care reliefează procedurile de lucru cu platforma, sunt prezentate date fictive, care nu au legătură cu realitatea ori cu persoane fizice sau juridice reale. De menționat că această platformă dispune de mecanisme de securitate, printre care autentificarea multifactor, care trebuie activată odată cu înrolarea.

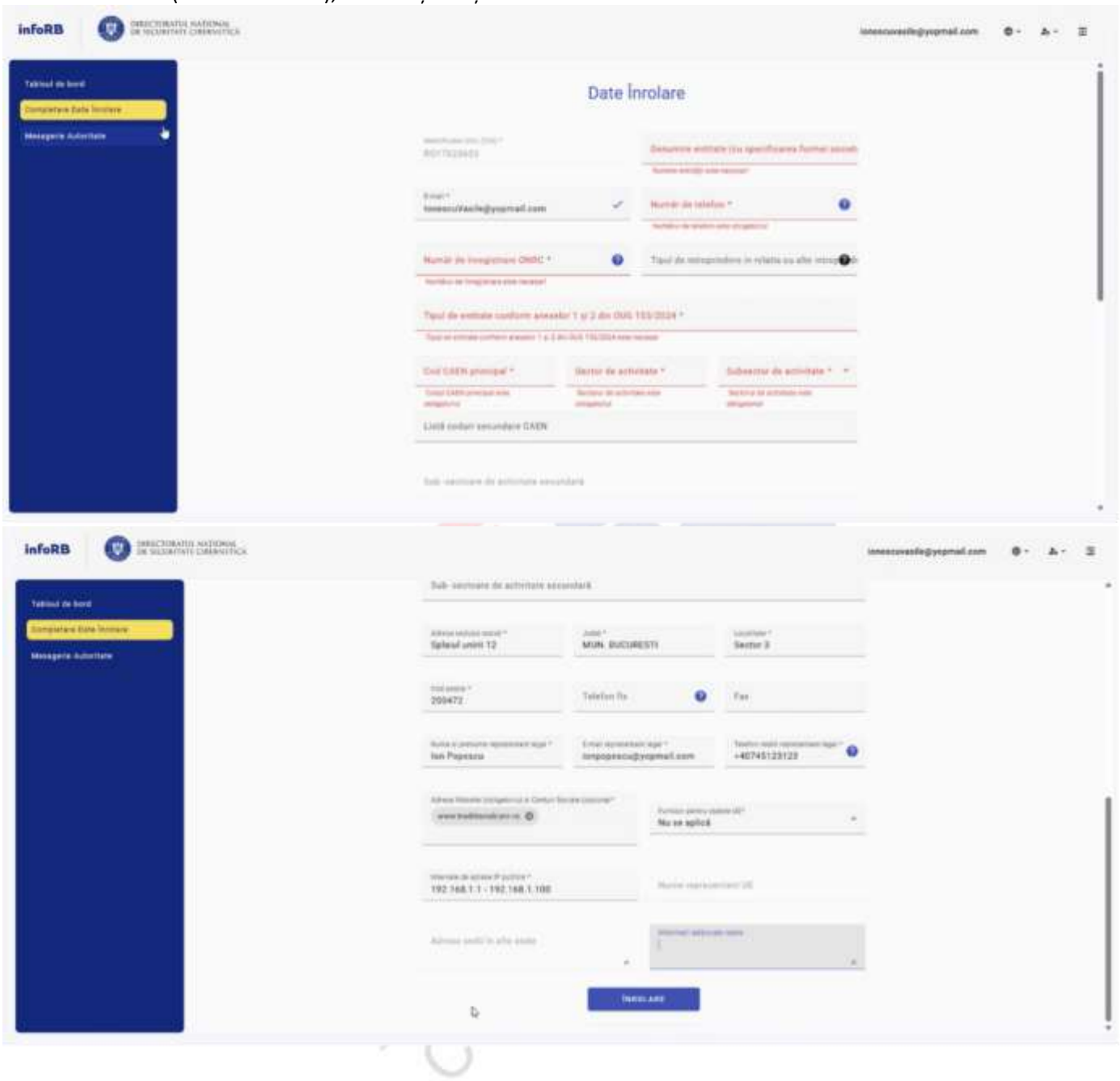


După parcurgerea acestui prim pas, cel de înrolare, trebuie parcurse etapele de identificare și clasificare, de evaluare de risc de securitate și se finalizează întregul proces cu evaluarea stării de maturitate a entității.



Se continuă cu completarea datelor de înrolare aparținând entității. Astfel, sunt menționate și unele câmpuri obligatorii, cum ar fi identificator unic (CUI), denumire, numărul de înregistrare în Registrul Comerțului, tipul de entitate, coduri CAEN principal și secundare (sunt prevăzute atât în varianta 2 cât și în varianta 3), sector și subsector de activitate, adresa sediului social, telefon, fax, numele, prenumele și datele de contact ale reprezentantului legal (care poate fi diferit de persoana desemnată pentru relația cu DNSC), adresa website-ului, dacă este furnizor pentru statele membre UE (se selectează dintr-un meniu de tip drop-down), adrese IP publice,

sedii în alte state (dacă este cazul), informații adiționale.



Validarea înrolării se efectuează după descărcarea documentului generat de aplicație, în format .pdf, asumarea acestuia de către reprezentantul legal al entității, cu ajutorul semnăturii electronice calificate, și încărcarea documentului semnat. Poate fi necesară încărcarea de documente justificative, conform cerințelor legale formulate.

ANEXA

NOTIFICARE

privind modificarea/completarea datelor responsabilului cu securitatea rețelelor și sistemelor informatice

A. Date generale (identificare entitate solicitantă)

DENUMIRE SOLICITANT: **SC Traditional Carn Srl**
ID Entitate: **RO17623633**
ADRESĂ CORESPONDENȚĂ
Adresa completă: **Splaiul unirii 12, +40745267192, IonescuVasile@yopmail.com**
Localitate: **Sector 3**/ județ: **MUN. BUCURESTI**

RESPONSABIL NIS: prenumele și Numele Ionescu Vasile , funcția în cadrul entității CISO, nr. telefon mobil(+) +40745267192, adresa de e-mail instituțională(+) IonescuVasile@yopmail.com

B. Solicitare

În temeiul Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, cu modificările și completările ulterioare, și a Legii nr. 58/2023 privind apărarea cibernetică solicităm:

☐ Înscrierea de modificări/completări referitoare la responsabilul desemnat în Lista entităților esențiale și importante

C. Acord prelucrare date [1]

Solicitantul își exprimă acordul cu privire la prelucrarea datelor cu caracter personal și procesarea electronică a datelor de către DNSC/ ANSRSI în procesul de implementare și monitorizare a Legii nr. 362/2018, cu modificările și completările ulterioare.

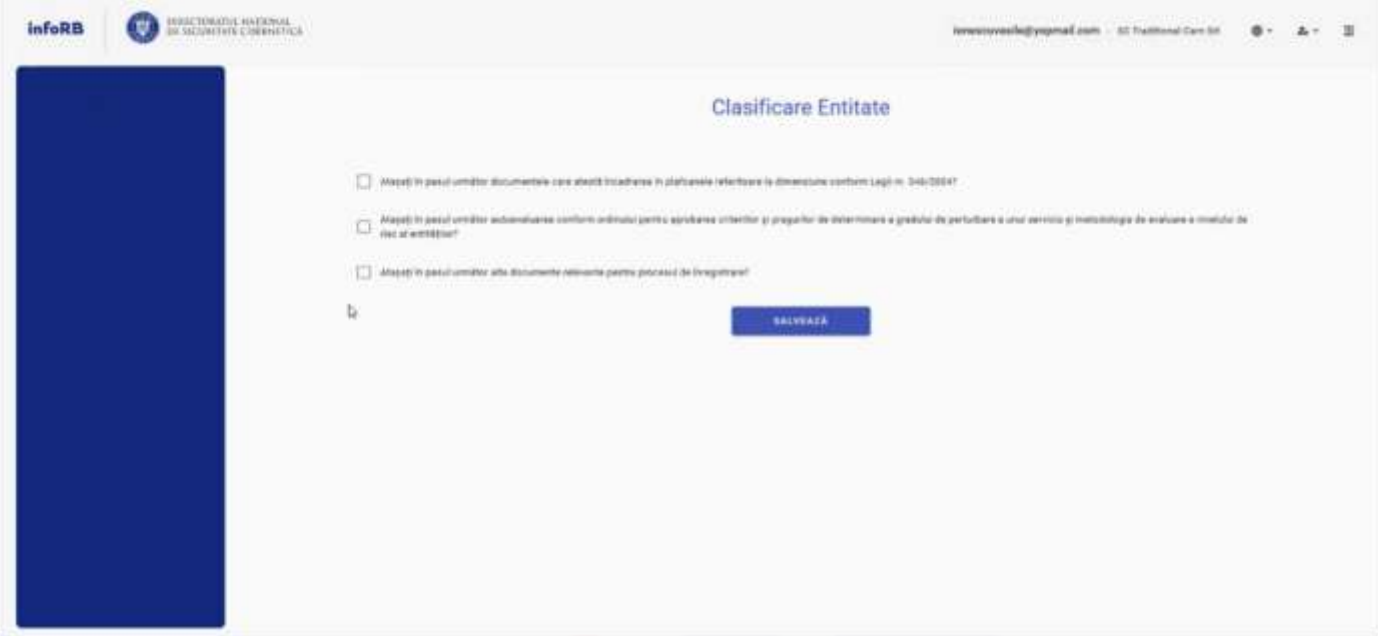
☐ Da

D. Documente anexate

☐ ..... , nr. ..... / (.....)
file

REPREZENTANT LEGAL,
Nume și prenume: **Ionescu Vasile**
Data curentă: 07/01/2025 08:11:38
Semnătură:

După aprobarea notificării de către backoffice-ul DNSC, se trece la identificarea entității candidate prin furnizarea unor date pe baza cărora se poate stabili cu exactitate clasificarea entității, cum ar fi cifra de afaceri, numărul mediu de salariați, valoarea activelor totale, indicele de mărime al organizației și se bifează situațiile specifice reale ale entității în opozabilitate cu prevederile legale invocate în formular. Pentru clarificări, aplicația explicitează vizual fiecare item la parcurgerea cu cursorul peste aceștia.



De asemenea, ca la etapa anterioară, de înrolare, la final se salvează documentul generat în această etapă în format .pdf, se asumă de către reprezentantul legal și se încarcă în aplicație, așteptându-se aprobarea acestuia de la nivelul DNSC.

Page 2 of 2

C. Etapa Clasificare

Ataşaţi în pasul următor documentele care atestă încadrarea în plafoanele referitoare la dimensiune conform Legii nr. 346/2004? (Ataşaţi documentele din care rezultă valorile introduse pentru numărul de angajaţi, cifra de afaceri şi valoarea activelor, precum şi dimensiunea entităţii pe care aţi selectat-o conform prevederilor Legii nr. 346/2004 privind stimularea înfiinţării şi dezvoltării întreprinderilor mici şi mijlocii.) : **Nu**

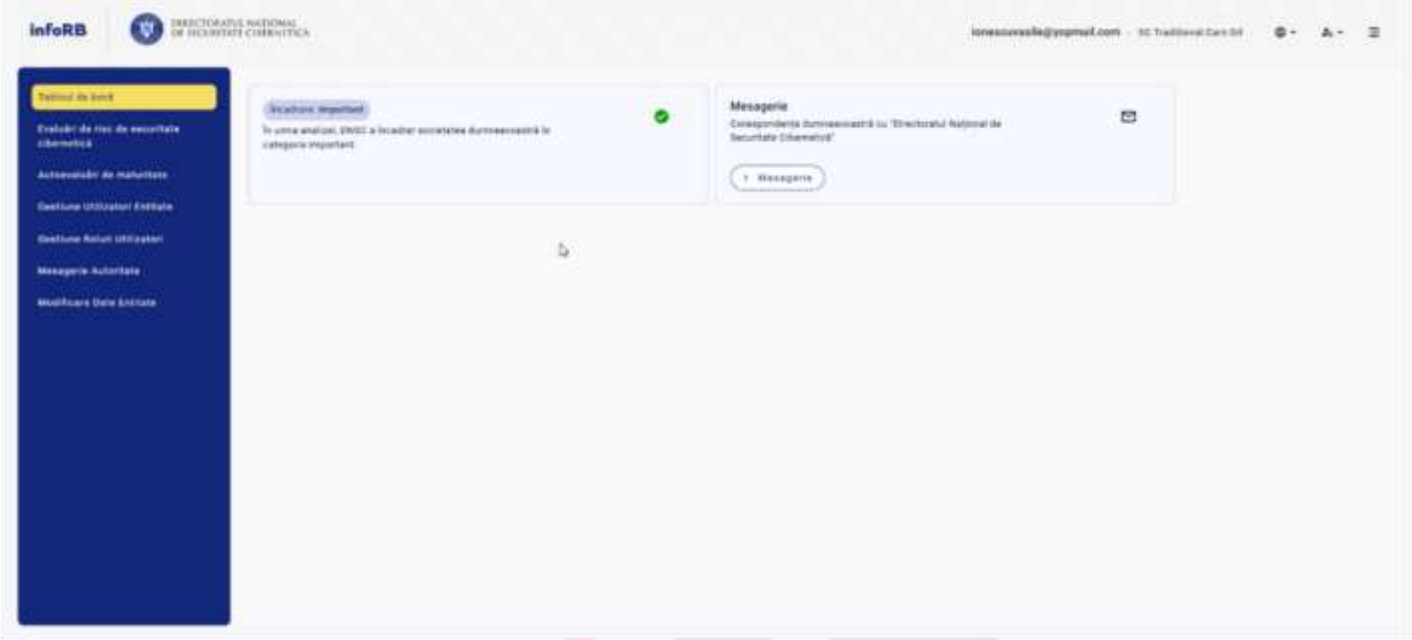
Ataşaţi în pasul următor autoevaluarea conform ordinului pentru aprobarea criteriilor şi pragurilor de determinare a gradului de perturbare a unui serviciu şi metodologia de evaluare a nivelului de risc al entităţilor? (Se ataşează autoevaluarea privind impactul generat de perturbarea serviciului pe care îl prestează entitatea dumneavoastră) : **Nu**

Ataşaţi în pasul următor alte documente relevante pentru procesul de înregistrare? (Aveţi de ataşat alte documente care atestă informaţiile introduse în platformă ca urmare a parcurgerii procesului de notificare până la această etapă) : **Da**

Rezultat: **Important**

Data curentă: 07/01/2025 08:13:33
Semnatură:

Odată cu finalizarea acestei etape de identificare și clasificare, în tabloul de bord al aplicației se poate vizualiza încadrarea entității ca esențială sau importantă, în urma analizei datelor și documentelor furnizate, în corelare cu domeniile din cadrul sectoarelor de activitate cuprinse în Anexele 1 și 2 din OUG 155/2024.

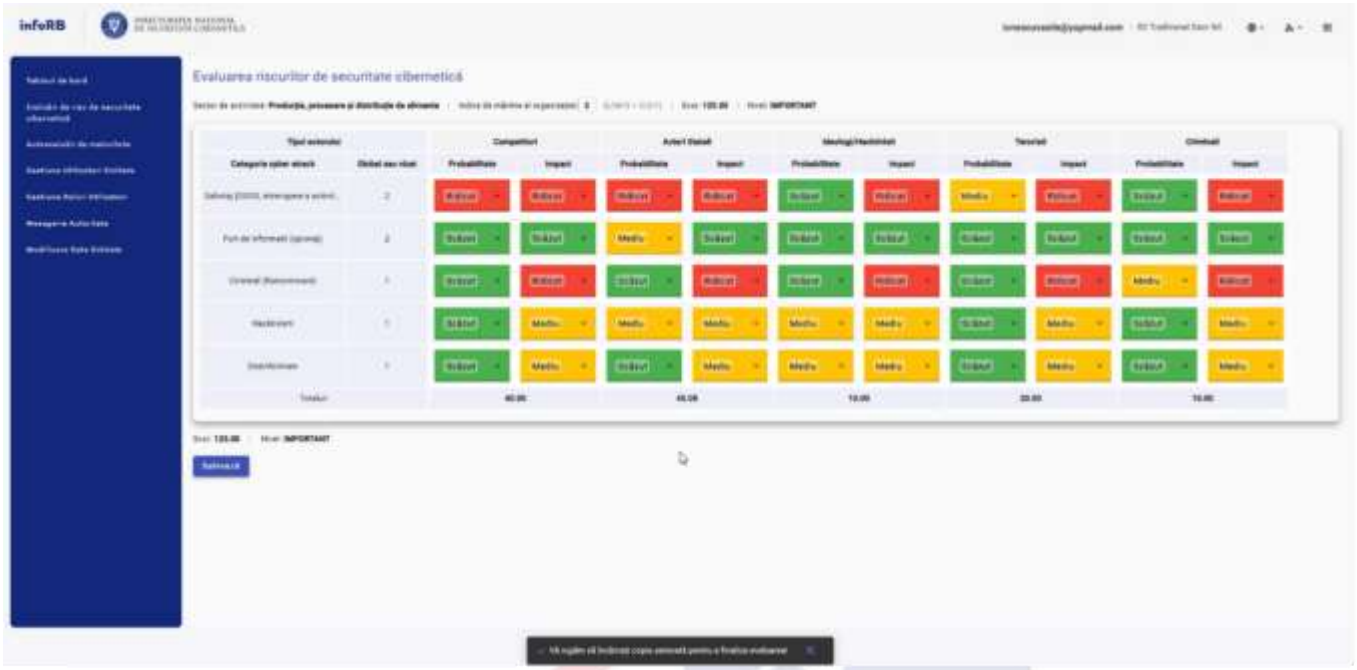


De reținut prevederea legală că **„atunci când o entitate desfășoară activitate în două sau mai multe sectoare, astfel cum sunt prevăzute în anexele nr. 1 și 2, acesteia i se aplică măsurile tehnice, operaționale și organizatorice proporționale și adecvate pentru a gestiona riscurile aferente securității rețelelor și a sistemelor informatice de nivelul cel mai ridicat**”. Este important acest aspect din punctul de vedere al următoarei etape, de evaluare a riscurilor de securitate cibernetică.

Procesul de evaluare a riscurilor de securitate cibernetică

Având în vedere dispozițiile art. 10 alin. (2) și ale art. 18 din Ordonanța de urgență a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil, DNSC urmează să adopte *„Ordinul pentru aprobarea criteriilor și pragurilor de determinare a gradului de perturbare a unui serviciu și metodologia de evaluare a nivelului de risc al entităților”*, aflat și acesta în etapa de proiect în Transparență decizională, pe site-ul directoratului.

Instrumentul de evaluare pus la dispoziție în cadrul acestei etape de experții DNSC, foarte bine realizat și ușor de utilizat, are la bază analize predefinite în funcție de sectorul de activitate al entității, care stabilește un scor ce determină clasificarea în urma evaluării. Scorul se modifică, în funcție de probabilitatea și impactul (scăzut, mediu sau ridicat) categoriilor de atacuri cibernetice principale vizate de evaluare (sabotaj, spionaj, criminalitate, hacktivism, dezinformare), ce pot fi derulate de diverse tipuri de actori (competitori, actori statali, ideologi/hacktiviști, teroriști, criminalitate cibernetică). Această evaluare ar trebui efectuată în corelare cu propriile analize de risc, entitățile putând să aducă modificări la parametrii predefiniți, astfel încât să reflecte cât mai fidel riscurile de securitate cibernetică la nivelul organizațiilor.



În mod asemănător etapelor anterioare, deja parcurse, raportul de evaluare a riscurilor se descarcă în format .pdf, se semnează electronic de către reprezentantul legal al entității și se încarcă în platformă.

Raport de Evaluare a Riscurilor

Scor Total al Evaluarii: 125.00
Clasificare in urma evaluarii:IMPORTANT

Evaluarea riscurilor cibernetice

Sabotaj (DDOS, intrerupere a activitatii...)

Competitori : Probabilitate : **Ridicat** Impact: **Ridicat**
Actori Statali : Probabilitate : **Ridicat** Impact: **Ridicat**
Ideologi/Hacktivisti : Probabilitate : **Scazut** Impact: **Ridicat**
Teroristi : Probabilitate : **Mediu** Impact: **Ridicat**
Criminali : Probabilitate : **Scazut** Impact: **Ridicat**

Furt de Informatii (spionaj)

Competitori : Probabilitate : **Scazut** Impact: **Scazut**
Actori Statali : Probabilitate : **Mediu** Impact: **Scazut**
Ideologi/Hacktivisti : Probabilitate : **Scazut** Impact: **Scazut**
Teroristi : Probabilitate : **Scazut** Impact: **Scazut**
Criminali : Probabilitate : **Scazut** Impact: **Scazut**

Criminal (Ransomware)

Competitori : Probabilitate : **Scazut** Impact: **Ridicat**
Actori Statali : Probabilitate : **Scazut** Impact: **Ridicat**
Ideologi/Hacktivisti : Probabilitate : **Scazut** Impact: **Ridicat**
Teroristi : Probabilitate : **Scazut** Impact: **Ridicat**
Criminali : Probabilitate : **Mediu** Impact: **Ridicat**

Hacktivism

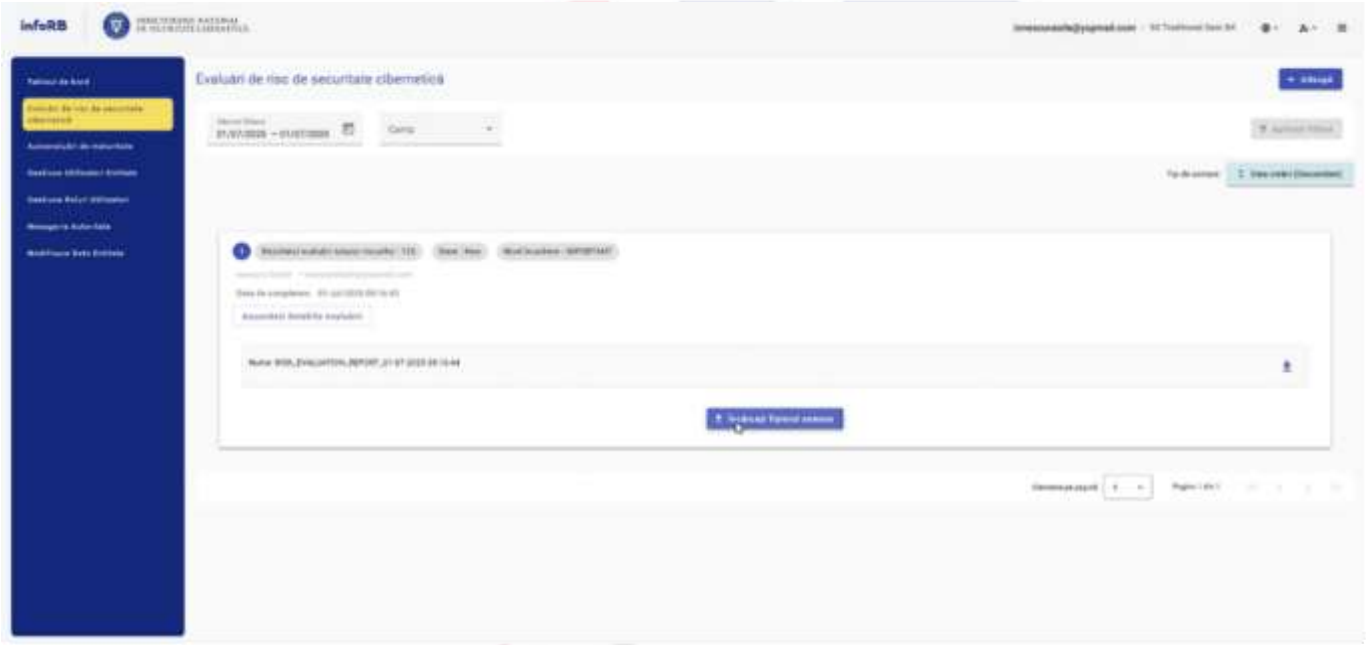
Competitori : Probabilitate : **Scazut** Impact: **Mediu**
Actori Statali : Probabilitate : **Mediu** Impact: **Mediu**
Ideologi/Hacktivisti : Probabilitate : **Mediu** Impact: **Mediu**
Teroristi : Probabilitate : **Scazut** Impact: **Mediu**
Criminali : Probabilitate : **Scazut** Impact: **Mediu**

Dezinformare

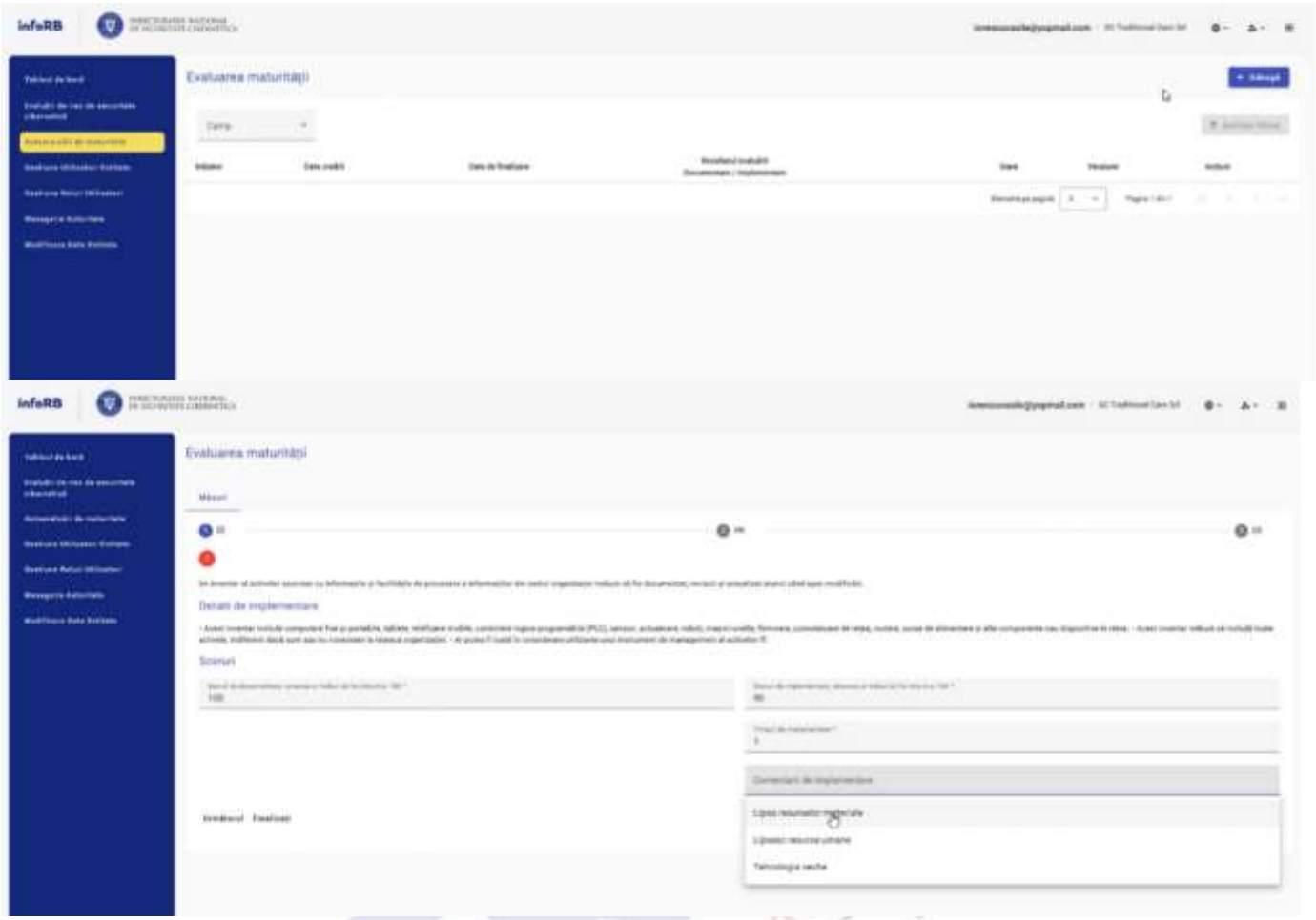
Competitori : Probabilitate : **Scazut** Impact: **Mediu**
Actori Statali : Probabilitate : **Scazut** Impact: **Mediu**
Ideologi/Hacktivisti : Probabilitate : **Mediu** Impact: **Mediu**
Teroristi : Probabilitate : **Scazut** Impact: **Mediu**
Criminali : Probabilitate : **Scazut** Impact: **Mediu**

Scor Total al Evaluarii: 125.00
Clasificare in urma evaluarii:IMPORTANT

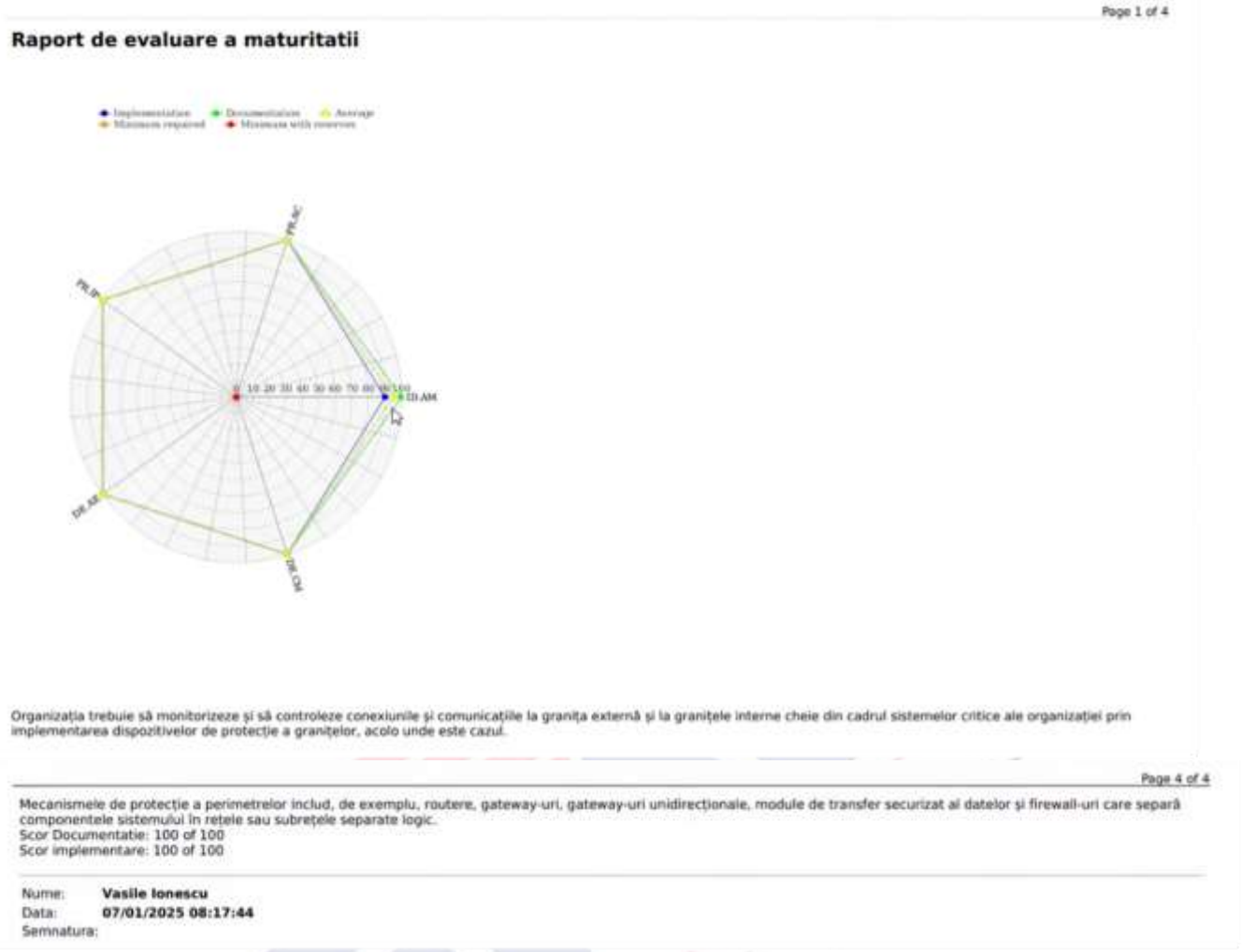
Nume si renume:	**Vasile Ionescu**
Data:	**01-07-2025**
Semnatura	



Următoarea etapă este cea a unei **autoevaluări de maturitate**, ce constă în parcurgerea unui chestionar ai căror itemi își schimbă culoarea din roșu în bleu, pe măsură ce sunt completați. Scorurile care se atribuie atât pe parte de documentare, cât și pe partea de implementare au valori cuprinse între 0 și 100. În situațiile în care scorurile nu au valoarea maximă, se cer date referitoare la timpul planificat de implementare integrală și motivele care au dus la diminuarea scorului (lipsa resurselor umane, lipsa resurselor materiale, tehnologia veche).



După finalizarea autoevaluării de maturitate, platforma generează un rezumat, iar dacă în urma revizuirii acestuia entitatea este de acord cu el se descarcă formatul .pdf, se asumă de reprezentantul legal, prin semnarea raportului de evaluare a maturității cu semnătură electronică calificată, și se încarcă documentul în platformă.



Page 1 of 4

Raport de evaluare a maturitatii

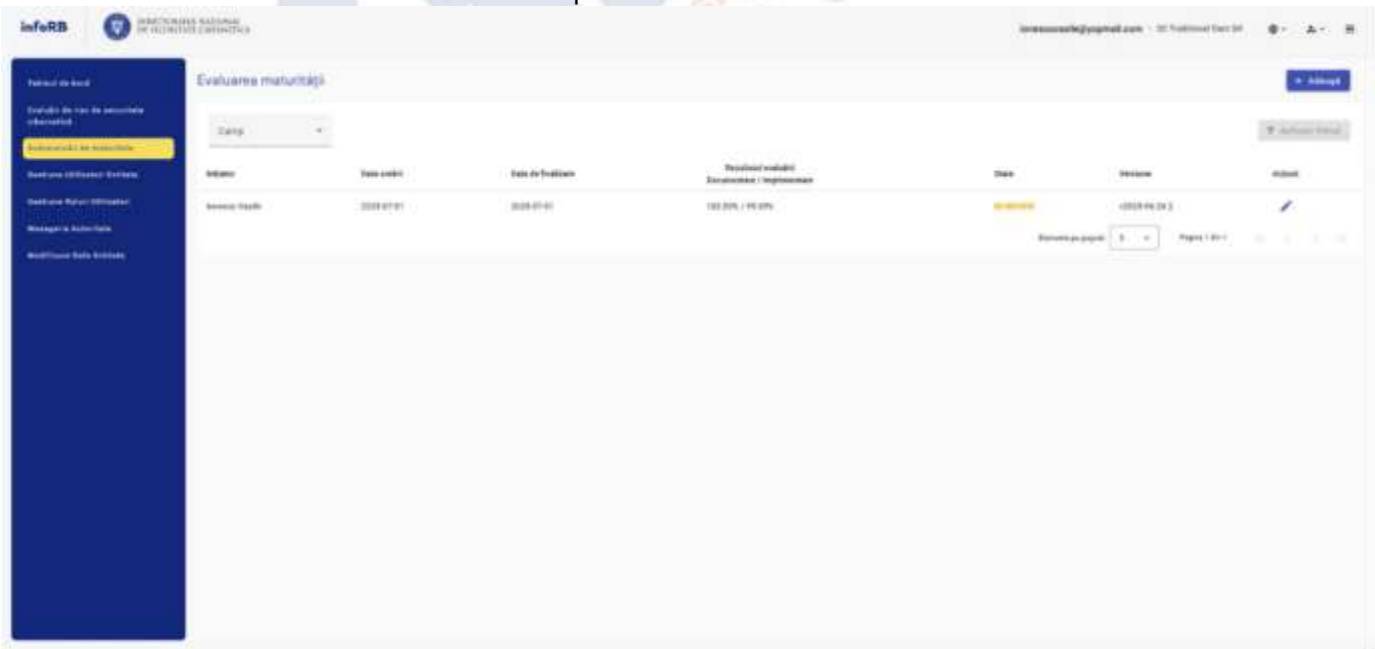
Organizația trebuie să monitorizeze și să controleze conexiunile și comunicațiile la granița externă și la granițele interne cheie din cadrul sistemelor critice ale organizației prin implementarea dispozitivelor de protecție a granițelor, acolo unde este cazul.

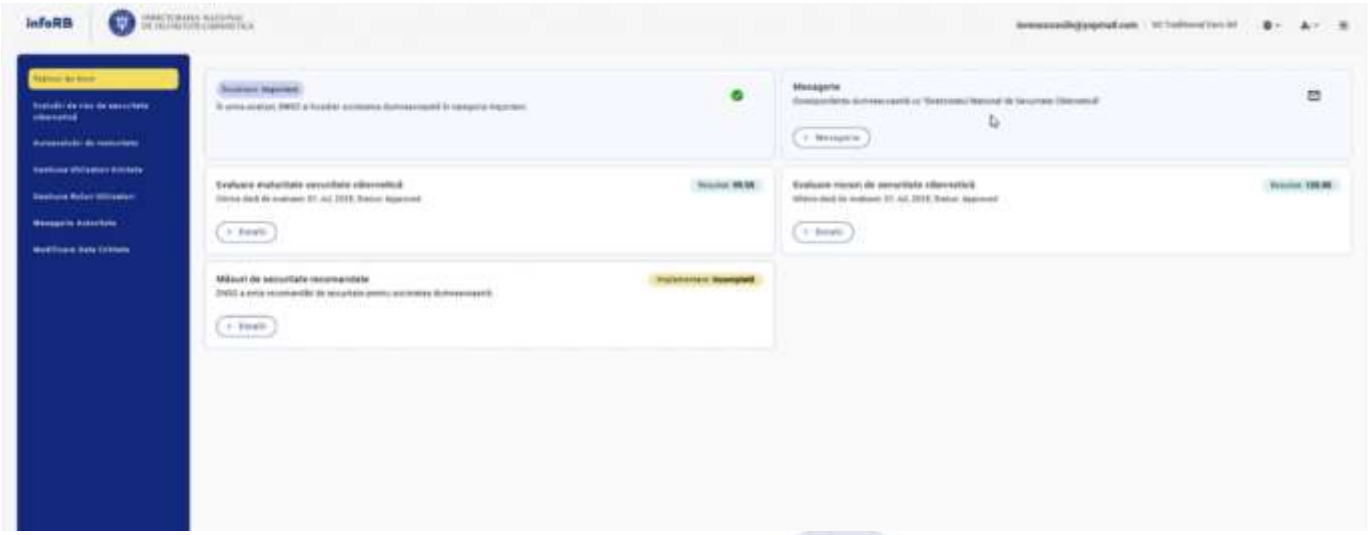
Page 4 of 4

Mecanismele de protecție a perimetrelor includ, de exemplu, routere, gateway-uri, gateway-uri unidirecționale, module de transfer securizat al datelor și firewall-uri care separă componentele sistemului în rețele sau subrețele separate logic.
Scor Documentatie: 100 of 100
Scor implementare: 100 of 100

Nume: **Vasile Ionescu**
Data: **07/01/2025 08:17:44**
Semnatura:

Starea evaluării maturității se poate urmări în tabloul de bord, documentul fiind revizuit de către DNSC, în baza căruia va emite recomandări de securitate pentru entitate.





Metoda principală de transmitere a formularelor de notificare este prevăzută a fi prin platformă. În situația indisponibilității platformei, transmiterea formularelor de notificare se efectuează prin poștă electronică. Dacă nu este disponibilă niciuna din metodele anterioare, se optează pentru depunerea fizică, pe suport hârtie, la sediul DNSC, astfel documentele pot fi semnate olograf de către reprezentantul/reprezentanții legal/i al/ai entității.
Urmează analizarea documentelor, informațiilor și datelor transmise de către entitate din perspectiva acurateței, exhaustivității, concludenței și pertinenței acestora iar în baza rezultatului evaluării se emite decizia de înregistrare a entității în registrul entităților și DNSC procedează la înregistrarea acesteia în registrul entităților.
În situația în care, în urma evaluării notificării, entitatea nu se încadrează în domeniul de aplicare al Ordonanței de urgență a Guvernului nr. 155/2024, aceasta nu se înregistrează în registrul entităților, urmând a fi notificată în acest sens.

Desigur, cele de mai sus reprezintă doar o scurtă prezentare a platformei, dezvoltate de către experții DNSC, pentru a veni în sprijinul entităților vizate și a înțelege mai ușor cum se desfășoară în practică procesul de notificare și de evaluare ce urmează a fi stabilit în curând prin Ordinele de implementare a OUG 155/2024, prezentarea detaliată și demonstrații tehnice ale funcționalităților platformei urmând a avea loc în cadrul unor evenimente viitoare organizate de specialiștii directoratului.
Impactul conformării pentru entitățile esențiale și importante
Conformarea nu înseamnă doar respectarea legii. Pentru multe companii, este o garanție de supraviețuire într-un mediu de afaceri în care încrederea între parteneri și a clienților față de entitățile furnizoare de servicii este vitală.
Beneficiile sunt evidente și, fără a fi exhaustivi, putem menționa câteva pe care le considerăm grăitoare pentru buna derulare a business-urilor entităților esențiale și importante
– reducerea semnificativă a riscului de breșe și atacuri cibernetice;
– scăderea probabilității unor sancțiuni financiare devastatoare;
– creșterea șanselor în derularea de contracte internaționale, în special cu entități care impun conformarea la NIS2 ca cerință contractuală;
– creșterea încrederii investitorilor și partenerilor comerciali.
Costurile implementării cerințelor de conformare și provocările în derularea continuă de activități specifice NIS2 nu sunt elemente de neglijat, organizațiile trebuind să le perceapă ca investiții și nu ca și cheltuieli, beneficiul pe termen lung, sesizat prin indicatorul ROI, fiind asigurarea permanentă a unui nivel corespunzător de securitate cibernetică, reducându-se astfel în mod semnificativ riscurile afectării business-ului.
Totuși, conformarea implică cheltuieli considerabile, mai ales pentru IMM-uri:
– investiții în tehnologie (firewalls, SIEM-Security Information and Event Management, EDR-Endpoint Detection & Response, DLP -Data Loss Prevention);
– contractarea de servicii MSSP- Managed Security Service Provider **sau consultanți specializați;**
– instruirea în mod regulat a personalului;
– audituri și teste periodice de penetrare.
Unele estimări internaționale arată că, pentru o entitate medie clasificată drept esențială, costurile de conformare pot reprezenta între 0,5% și 2% din cifra de afaceri anuală – o cifră semnificativă, dar adesea mai mică comparativ cu

costul unui singur incident cibernetic major. „Pentru societățile care s-ar încadra în domeniul de aplicare al cadrului NIS, se estimează că acestea ar avea nevoie de o creștere de maximum 22 % a cheltuielilor lor actuale în materie de securitate TIC pentru primii ani de la introducerea noului cadru NIS (aceasta ar fi de 12 % pentru societățile care intră deja sub incidența actualei Directive NIS). Totuși, această creștere medie a cheltuielilor în materie de securitate TIC ar conduce la un beneficiu proporțional al unor astfel de investiții, în special datorită unei reduceri considerabile a costurilor aferente incidentelor de securitate cibernetică (estimate la 118 miliarde EUR pe o perioadă de zece ani)”.

Riscurile și consecințele neconformării
În lipsa conformării, riscurile sunt uriașe, nu doar din perspectiva amenzilor. În lumea reală, costurile unui atac cibernetic se multiplică prin:
– amenzi de milioane de lei;
– costuri de remediere (recuperare date, consultanță juridică, PR de criză);
– procese civile din partea clienților sau partenerilor afectați;
– pierderea reputației și scăderea dramatică a valorii brandului.
Acestea demonstrează cât de rapid se poate transforma un incident de natură tehnică într-o criză socială și economică de proporții, cu impact ce poate deveni cu ușurință unul transfrontalier.

Concluzii și recomandări
Adoptarea Legii nr. 124/2025 și implementarea Directivei NIS2 reprezintă un moment de cotitură pentru securitatea cibernetică în România.
Entitățile vizate trebuie să înțeleagă că **decizia de a acționa rapid este singura cale sigură, în primul rând în implementarea unui ecosistem de securitate cibernetică și în al doilea rând, în vederea conformării, urmărind în principal:**
– să realizeze un audit complet asupra infrastructurii și proceselor, apelând la serviciile unor auditori atestați de DNSC;
– să investească în tehnologii moderne, precum și în atragerea și retenția de oameni bine pregătiți în domeniul securității cibernetice;
– să folosească instrumentele puse la dispoziție de DNSC pentru autoevaluare și notificare precum și, ulterior, să urmărească procesul de elaborare a celorlalte acte normative subsecvente domeniului;
– să stabilească și să aplice politici clare de răspuns la incidente;
– să comunice transparent cu autoritățile și cu partenerii.
Într-o lume unde un atac cibernetic poate produce consecințe comparabile cu un dezastru natural sau poate deveni chiar un act de război, conformarea cu NIS2 și legislația națională nu mai este o opțiune, ci o necesitate vitală.