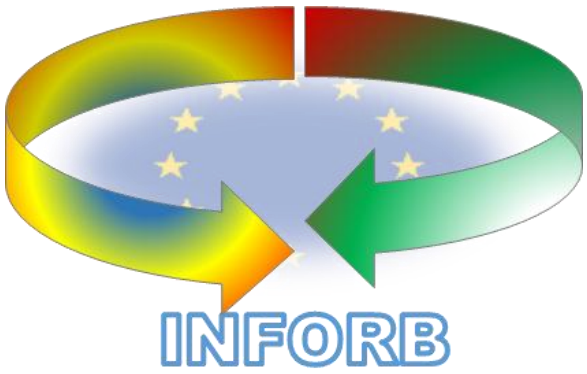

PLATFORMA DE COOPERARE NAȚIONALĂ ȘI TRANSFRONTALIERĂ NIS – ROMÂNIA ȘI BULGARIA [CORB].

LIVRABIL D3.1

Versiunea 1.0

REZUMAT

Livrabilul D3.1 "Platforma pentru cooperare națională și transfrontalieră NIS – România și Bulgaria [CORB]" detaliază viziunea, cerințele și designul la nivel înalt al platformei unificate de evaluare, notificare și schimb de informații privind securitatea cibernetică, sprijinind părțile interesate din sectorul alimentar din România și Bulgaria să îndeplinească obligațiile Directivei NIS2, permițând evaluarea unificată a securității cibernetice, notificarea incidentelor și schimbul transfrontalier securizat de informații. Începe prin cartografierea actorilor cheie (OES/IE, CERT naționale, autorități de reglementare) și fluxurile lor de lucru de schimb de informații, apoi specifică cerințele operaționale, de securitate și de confidențialitate a datelor. Acesta prezintă arhitectura modulară a platformei – separând serviciile naționale de cele transfrontaliere – și detaliază componentele de bază (autentificare, tablou de bord de raportare, interfețe API, straturi de criptare). În cele din urmă, prezintă un plan de validare a testelor funcționale și de securitate.

INFORMAȚII PRIVIND CONTROLUL DOCUMENTELOR

Setări	Valoare
Titlul documentului:	Platforma de cooperare națională și transfrontalieră NIS – România și Bulgaria [CORB]
Numărul proiectului:	101128047
Nume proiect:	Implementarea Directivei NIS în sectorul producției, procesării și distribuției de alimente din România și Bulgaria.
Acronimul proiectului:	INFORB
Autor(i) Document:	Josef KALLEDER (DNSC) Cătălin LUMEZANU, Ionuț CIOBANU, Anca BOGDAN (Certsign); Viorel HORGA, Alin IACOBAN, Tiberiu BARABOI (Expertware)
Identificator livrabil:	D3.1
Data scadentă a livrării:	31.07.2025
Data livrării:	31.07.2025
Manager de proiect:	Constantin CĂLIN
Versiunea documentului:	V1.0
Sensibilitate:	PU-Public
Dată:	30.07.2025

Evaluatori și evaluatori de documente

Nume	Rol	Acțiune	Dată
Josef KALLEDER	Liderul WP 3	Proiect de document creat	15.05.2025
Josef KALLEDER	Liderul WP 3	Versiunea originală (DNSC)	15.07.2025
Cătălin LUMEZANU	Șef de echipă/Arhitect software/Dezvoltator software	Actualizați versiunea (CERTSIGN)	25.07.2025
Tiberiu BARABOI	Consilier tehnic	Actualizați versiunea (EXPERTWARE)	26.07.2025
Consiliul consultativ de experți	Evaluare	Versiune convenită	30.07.2025
Constantin CĂLIN	Manager de proiect	Documentul final aprobat și livrat	31.07.2025

Istoricul documentelor

Revizie	Dată	Creat de	Scurtă descriere a modificărilor
V0	15.05.2025	Liderul WP 3	Document creat
V0.1	15.06.2025	Liderul WP 3	Rectificarea documentului actualizat cu informații
V0.1.1	15.07.2025	Liderul WP 3	Limba engleză actualizată
V0.1.2	25.07.2025	Șef de echipă/Arhitect software/Dezvoltator software	Limba engleză actualizată de CERTSIGN
V0.1.3	26.07.2025	Consilier tehnic	Limba engleză actualizată de experții bulgari
V1.0	30.07.2025	Liderul WP 3	Documentul final versiunea 1

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

Cuprins

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

SECȚIUNEA 1. PLATFORMA DE COOPERARE INFORB. REZUMAT

Cheie	Descriere
Obiectiv principal	Proiectarea și implementarea unei platforme web partajate, scalabile, cloud-native care să permită colaborarea în timp real între autoritățile de securitate cibernetică din România (DNSC) și Bulgaria (MEG-BG) și entitățile din sectorul alimentar, asigurând conformitatea cu obligațiile NIS2, inclusiv clasificarea, autoevaluarea, raportarea incidentelor și coordonarea transfrontalieră. Sistemul sprijină (1) identificarea și clasificarea entităților esențiale/importante, (2) schimbul bidirecțional de date cu fiecare autoritate națională și (3) coordonarea transfrontalieră de la autoritate la autoritate, astfel cum este stabilită prin acordul de grant.
Beneficiari principali	*Direct*: • **Autorități naționale competente (DNSC RO, MEG-BG)** — entități de înscriere în țările respective, supravegherea sectorului și statistici. • **Entități din sectorul alimentar (producători, procesatori, distribuitori) clasificate ca esențiale sau importante** – conformitate și managementul riscurilor. *Indirect:* • **Consumatori și parteneri din lanțul de aprovizionare care beneficiază de o rezistență cibernetică mai puternică**.
Funcționalități cheie	**Îmbarcare ghidată** – flux multilingv (RO/EN/BG) care permite introducerea datelor companiei și aplică reguli de clasificare **Autoevaluări de risc și maturitate** — chestionare mapate NIS 2 cu scor automat și urmărire a istoricului **Motor de recomandare** — leagă scorurile de acțiunile de remediere și de captarea costurilor **Mesagerie securizată & Document Hub** — conversații între entități și autorități, plus canal peer de la autoritate la autoritate **Tablouri de bord și rapoarte** - analize la nivel de sector, export de date structurate și widget-uri pentru management și utilizare în politici **Nucleu de securitate întărit** — 2FA în locuri critice, acreditări hash, administrator restricționat prin IP/VPN, jurnale complete de audit al acțiunilor utilizatorului
Rezultate așteptate	**Conformitate mai rapidă** – în înregistrarea entităților din sectorul alimentar, inclusiv completarea a cel puțin o autoevaluare digitală, conform legii. **Informații transfrontaliere** – canal pentru informații comune despre sectorul RO/BG care alimentează conștientizarea situației la nivelul UE. **Difuzarea cunoștințelor** — ≥ 150 de descărcări publice ale rezultatelor proiectului pe care le găzduiește modulul public al platformei **Risc redus** – scădere măsurabilă a constatărilor cu severitate ridicată în evaluările succesive (țintă ≥ reducere de 20 %)

Pe scurt, platforma INFORB oferă un instrument unic și sigur în care autoritățile și operatorii din sectorul alimentar pot clasifica, evalua și monitoriza postura de securitate cibernetică - la nivel național și pot împărtăși informații critice peste granița RO-BG - oferind o reducere tangibilă a riscurilor și o conformitate simplificată cu NIS 2.

SECȚIUNEA 2. STRUCTURAREA DETALIATĂ A ACTIVITĂȚILOR

WP3	Dezvoltarea unei platforme de informare și cooperare	
T3.1	Dezvoltarea cerințelor operaționale pentru dezvoltarea platformei de cooperare CORB.	Definirea obiectivelor, structurii cerințelor și experților. Documentarea cerințelor funcționale și nefuncționale, precum și a cerințelor de performanță.
		Dezvoltarea diagramelor, schițelor și interfețelor necesare funcționării platformei.
		Stabilirea cerințelor de securitate și a tehnologiilor utilizate pentru dezvoltarea platformei CORB.
		Definirea și stabilirea cooperării dintre dezvoltator și reprezentantul beneficiarului.
		Stabiliți cerințele de testare și validare ale platformei, precum și cele de revizuire, aprobare, actualizare și managementul modificărilor.
T3.2	Dezvoltare și operaționalizare "Platformă pentru cooperare națională și transfrontalieră NIS – România și Bulgaria [CORB]".	Stabilirea și expunerea principiilor și practicilor utilizate de beneficiar și de dezvoltatorul platformei pentru livrarea unui produs de înaltă calitate.
		Gestionați și prioritizați lista de specificații ale platformei, asigurați o comunicare deschisă în procesul de dezvoltare a platformei și identificați toate soluțiile pentru livrarea unei platforme conforme.
		Întâlniri periodice între reprezentantul beneficiarului și echipa de dezvoltare a platformei CORB.
		Asigurarea faptului că o versiune funcțională și testabilă a platformei este livrată la sfârșitul fiecărui sprint, precum și la sfârșitul dezvoltării.
T3.3	Testarea și validarea platformei de cooperare CORB.	Efectuați teste regulate ale platformei dezvoltate pentru a asigura calitatea și funcționalitatea continuă a software-ului.
		Dezvoltarea de către dezvoltator a unui raport de testare pentru fiecare sprint și lansare (conține: scenarii de testare, rezultate ale testelor și situații emergente și va fi pus la dispoziție printr-un sistem de management al testelor).
		Validarea testelor și solicitarea de scenarii de testare suplimentare pentru atingerea scopurilor testului. Validarea pentru fiecare funcționalitate livrată a existenței documentației tehnice a codului și actualizarea documentației de întreținere, migrare, scalare și interconectare referitoare la funcționalitatea respectivă și la sistem în ansamblu.
		Validarea funcționalității și performanței platformei. Evaluarea securității. Testarea capacității și ușurinței de operare a platformei.

Concluzie

Activitățile din WP 3 au stabilit o cale clară de la concept la o platformă de cooperare CORB validată. T3.1 a definit obiectivele, cerințele și normele de guvernanță; T3.2 le-a transformat în software funcțional prin sprinturi agile cu feedback continuu al beneficiarilor; și T3.3 au verificat fiecare increment prin teste riguroase, verificări de securitate și verificări ale documentației.

Împreună, cele trei sarcini au format un ciclu iterativ – definirea → dezvoltarea → validarea → perfecționarea – care a redus riscul tehnic și a menținut platforma aliniată la nevoile și reglementările părților interesate. Până la sfârșitul WP 3, consorțiul a livrat o platformă pregătită pentru producție, complet documentată, cu un model de guvernanță care sprijină schimbările viitoare, oferind o bază solidă pentru implementare, colaborare transfrontalieră și sustenabilitate pe termen lung.

SECȚIUNEA 3. CERINȚE OPERAȚIONALE ȘI TEHNICE

Acest capitol prezintă principalele cerințe operaționale și tehnice care au fost elaborate pentru dezvoltarea, implementarea și operarea cu succes a platformei.

3.1. Cerințe operaționale

3.1.1. Părțile interesate și rolurile utilizatorilor

Platforma deservește trei grupuri principale de utilizatori:

- **Entități (esențiale/importante/voluntare):** organizații desemnate în temeiul NIS2 ca entități esențiale sau importante sau cele care optează pentru alinierea voluntară la directivă.
- **Autorități (DNSC în România, MEGBG în Bulgaria):** responsabile cu supravegherea, analiza riscurilor și validarea conformității.
- **Publicul larg:** furnizarea de informații, metodologii și orientări pentru sectorul în general.

Pentru entitate și autoritate, fiecare tip de utilizator are roluri și permisiuni diferențiate, inclusiv administratori, ofițeri de conformitate, reprezentanți ai entităților și așa mai departe. Permisiunile de utilizator sunt detaliate, acoperind drepturile de citire/editare pentru module precum integrarea, evaluarea riscurilor, evaluările maturității și comunicațiile.

3.1.2. Procese funcționale de bază

- **A fost implementată integrarea și validarea** entităților prin introducerea automată (bazată pe API) și manuală a datelor. Cu toate acestea, din cauza lipsei de fiabilitate a platformei terțe care ar fi trebuit să ne servească datele, platforma se bazează în prezent pe introducerea manuală a datelor, stabilizarea în așteptare și respectarea SLA de la furnizorul de date terț (adică ONRC).
- **Identificarea și clasificarea entităților** a fost implementată folosind un mecanism de reguli și criterii configurabile. Am configurat astfel de reguli conform cerințelor legislației actuale, dar există mecanisme pentru a face actualizarea simplă în cazul în care legea va evolua în viitor.
- **Autoevaluarea maturității securității cibernetice și a expunerii la riscuri** a fost implementată folosind șabloane predefinite personalizabile grupate în seturi controlate cu versiuni. Pentru personalizarea versiunii de producție, am utilizat măsurile de risc și maturitate prevăzute în legislația aplicabilă în prezent.
- **Fluxuri de lucru** de comunicare între entități și autorități, inclusiv schimbul de fișiere.
- **Gestionarea documentelor** și arhivarea declarațiilor, evaluărilor și justificărilor, după cum este necesar.

3.1.3. Operaționalizarea transfrontalieră

Fiecare țară (România și Bulgaria) va avea propria instanță a platformei, care rulează pe infrastructură și baze de date separate. Interoperabilitatea este asigurată prin sisteme de mesagerie peer-to-peer pentru coordonarea între autorități.

3.2. Cerințe tehnice

3.2.1. Arhitectura aplicației

- **Aplicație bazată pe web, pregătită pentru cloud,** accesibilă prin browser bazate pe Chromium.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

- Construit folosind **.NET Core 8.0**, **AngularJS 17.3.1** și **NodeJS 18**.
- Găzduit pe **containere Docker** care rulează **Debian 11/12**.
- Folosește **MSSQL 2022** ca motor de baze de date.
- **WordPress CMS** este utilizat pentru gestionarea site-ului web informațional orientat spre public.

3.2.2. Autentificare și autorizare

- **Se integrează cu un serviciu** central PAUT (autentificare și autorizare) **pentru conectare securizată.**
- **Impune** 2FA (autentificare cu doi factori) **pentru toți utilizatorii.**
- **Politicile de parolă necesită lungime minimă, complexitate și reînnoire periodică.**
- **Implementează controale de acces la nivel de rețea,** inclusiv lista albă IP și restricțiile VPN pentru endpoint-urile administrative backend**.**
- Implementează controlul accesului bazat pe roluri (RBAC) **cu scheme de permisiuni configurabile.**
- **Toate operațiunile sensibile sunt înregistrate pentru audit**
- **Anumite operațiuni critice necesită o** confirmare suplimentară a MFA**.**

3.2.3. Controale de securitate cibernetică

- Parolele sunt stocate folosind algoritmi de hashing criptografic standard din industrie, cum ar fi Argon2, cu mecanisme de sare și piper aplicate.
- Gestionarea securizată a sesiunii folosind cookie-uri și mecanisme de expirare.
- Igienizare riguroasă **a intrărilor** pentru a preveni atacurile de injecție.
- Controlul versiunilor pentru modelele de risc și maturitate pentru a asigura audibilitatea și conformitatea cu reglementările.

3.2.4. Modelul și integritatea datelor

- Tastare și validare puternică a datelor (de exemplu, standardul E.123 pentru numerele de telefon, validarea formatului IBAN).
- Toate înregistrările includ metadate de trasabilitate: created_by, updated_by, marcaje temporale.
- **Mecanismele de ștergere temporară** asigură că datele nu se pierd niciodată, chiar și atunci când sunt eliminate logic din interfața de utilizare.

3.2.5. Interoperabilitate și extensibilitate

- Interfețe cu servicii externe (ONRC) folosind API-uri RESTful. În prezent dezactivat din cauza timpului de răspuns ONRC nesigur.
- Importă și exportă date prin .csv șabloane pentru operațiuni în lot.
- Interfață localizată în **română, engleză și bulgară**.

3.2.6. SLA și confidențialitate

- Fiecare instanță (România, Bulgaria) este izolată, asigurând suveranitatea datelor.
- Drepturile de acces și nivelurile de confidențialitate a datelor sunt controlate pe rol și pe afiliere organizațională.

- Sunt menținute piste de audit cuprinzătoare pentru toate operațiunile critice, cu mecanisme de înregistrare și politici de păstrare care susțin analiza criminalistică post-incident și raportarea de reglementare.

Concluzie

Secțiunea 3 a distilat condițiile prealabile operaționale și tehnice care au stat la baza realizării cu succes a platformei de cooperare CORB. Din punct de vedere operațional, am clarificat rolurile părților interesate, am atribuit permisiuni fine și am cartografiat procesele de bază - de la integrare și autoevaluare a maturității până la coordonarea transfrontalieră - care au permis utilizarea eficientă de zi cu zi.

Din punct de vedere tehnic, am definit o arhitectură containerizată pregătită pentru cloud, construită pe .NET Core 8.0 și Angular 17, securizată de autentificare PAUT centralizată, controale multifactoriale și măsuri riguroase de securitate cibernetică, cum ar fi hashing-ul parolelor Argon2 și înregistrarea cu evidență a falsificării. Un model de date strict și auditabil a păstrat integritatea și suveranitatea pentru instanțele separate din România și Bulgaria, în timp ce localizarea, interfețele API și SLA-urile clar limitate au asigurat extensibilitatea și conformitatea pe termen lung.

Împreună, aceste cerințe au format un plan detaliat care a condus dezvoltarea, a minimizat riscul de implementare și a asigurat că sistemul livrat îndeplinește atât mandatele de reglementare, cât și nevoile operaționale practice.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

SECȚIUNEA 4. ARHITECTURA SISTEMULUI

Platforma CORB este proiectată ca o aplicație web modulară, pregătită pentru cloud. Arhitectura sa pune accentul pe scalabilitate, suveranitatea datelor, securitatea și interoperabilitatea.

4.1. Prezentare generală a arhitecturii la nivel înalt

Platforma este compusă din:

- **Interfață**: aplicație web pentru utilizatori publici, entități și administratori.
- **Backend (strat API):** Servicii RESTful care gestionează logica, autentificarea și integrarea.
- **Micro-servicii**:
  - Autentificare și autorizare (PAUT)
  - Serviciu de semnare la distanță (RSS)
  - Motor de notificare
  - Motor de raportare
  - Motor de mesagerie internă entitate-autoritate
- **Strat de date**: instanțe de bază de date MSSQL 2022, una pentru fiecare instanță de țară.
- **Zona publică**: CMS WordPress pentru conținut informațional (conținut static, întrebări frecvente, metodologii, ghiduri de bune practici etc).
- **Motor de mesagerie** transfrontalieră: Mesagerie criptată peer-to-peer între autorități.

Implementarea este containerizată folosind Docker și orchestrată folosind Docker Compose, găzduită pe sisteme bazate pe Debian pentru a asigura scalabilitatea modulară, izolarea defecțiunilor și operațiunile DevSecOps simplificate.

4.2. Modelul de implementare și interconectivitate

Fiecare țară operează o **desfășurare complet izolată**:

Exemplu	Țara gazdă	Autoritate	Bază de date	Codul aplicației
INFORB-RO	România	DNSC	MSSQL RO DB	Bază de cod partajată
INFORB-BG	Bulgaria	MEGBG	MSSQL BG DB	Bază de cod partajată

Baza de cod partajată asigură consecvența funcționalității, în timp ce parametrizarea stocată în baza de date permite ajustări regionale (cataloage, limbă, reglementări, taxonomie).

Nu există infrastructură sau bază de date comună între țări, asigurând **suveranitatea datelor**. Sistemele inter-operează prin schimbul securizat de mesaje.

4.3. Prezentare generală a modelului de date

Platforma implementează un model de date relațional conceput pentru:

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

- **Gestionarea utilizatorilor și a rolurilor**: mai multe roluri de utilizator folosind schema RBAC, MFA, jurnale de activitate.
- **Profiluri de entitate**: date despre companii, clasificarea sectorului alimentar, date de contact ale persoanelor asociate.
- **Date de identificare și clasificare: răspunsuri la criteriile IDC, dimensiunea entității, numărul de angajați, valoarea activelor și cifra de afaceri.**
- **Evaluarea riscurilor și a maturității**: chestionare diferite versiuni, logică de evaluare, justificări, recomandări.
- **Nomenclator:** tabele de căutare centralizate (de exemplu, actori de amenințări, categorii de impact, controale de securitate).
- **Cataloage** coduri NACE, orașe și orașe naționale, tipuri de entități etc.
- **Jurnale de audit și mesagerie**: trasabilitate completă a acțiunilor, firelor de comunicare și schimburilor de documente.

Toate entitățile principale includ:

- ID unic
- Marcaje temporale (create, actualizate)
- Metadate utilizator (created_by, updated_by)
- Steaguri de ștergere temporară

4.4. Arhitectura comunicațiilor și securității

4.4.1. Comunicații interne ale sistemului

Toate modulele interne (frontend, backend, servicii) comunică folosind autentificarea securizată bazată pe HTTPS și OAuth prin PAUT.

- **Gestionarea sesiunii**: cookie-uri securizate, timeout-uri de sesiune
- **Protecția** datelor: validare intrare, protecție XSS/CSRF, atenuare injecție SQL
- **Jurnale de audit**: urmărirea tuturor acțiunilor utilizatorilor

4.4.2. Integrări externe

Sistem extern	Tip de interfață	Scop
ONRC	API REST (opțional)	Pre-completarea datelor de entitate prin CUI (suspendată în prezent)
CertSIGN PAUT	OAuth / REST	Identitate utilizator, 2FA, resetare parolă
CertSIGN RSS	Protocolul CSC	Semnătură electronică (încărcări PDF)
Gateway-uri de e-mail/SMS	SMTP/REST	Notificări și livrare MFA

4.5. Mecanismul de comunicare transfrontalieră

Pentru a asigura coordonarea în timp real între autoritățile române și bulgare, platforma include un **modul de mesagerie transfrontalieră**. Caracteristici cheie:

- **Cozi de mesaje asincrone**
- **Sarcini utile criptate**
- **Rutarea mesajelor se realizează prin servicii de gateway securizate care acceptă autentificarea reciprocă, criptarea end-to-end (TLS 1.3 sau o versiune ulterioară) și trasabilitatea în scopuri de audit de reglementare.**

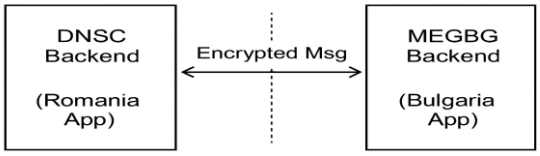

Figura 1. Diagramă: Interacțiunea transfrontalieră.

- **Subiecte bazate pe subiecte**

Fiecare autoritate își menține propriile jurnale, sesiuni de utilizator și înregistrări, în timp ce firele și rapoartele selectate sunt partajate prin puncte finale controlate.

4.6. Scalabilitate și extensibilitate

- **Arhitectura dockerizată** permite implementarea modulară și scalarea orizontală.
- **Controlul versionat** al modelelor de risc și scadență permite adaptarea la actualizările de reglementare.
- **Sistemul de nomenclator** acceptă extinderea ușoară cu noi sectoare, reguli sau logică de notare care se adaptează evoluției viitoare a legislației.
- **Suportul multi-lingv** este integrat prin fișiere de localizare (RO, EN, BG).

4.7. Diagramă: Arhitectura platformei (simplificată)

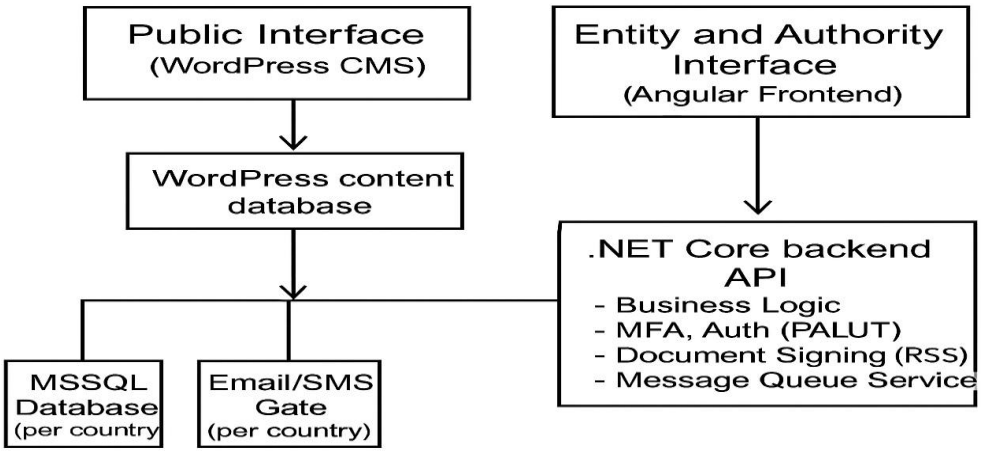

Figura 2. Diagramă: Arhitectura platformei (simplificată).

Această arhitectură asigură o colaborare sigură, conformă și eficientă peste granițele naționale, păstrând în același timp autonomia datelor fiecărei țări și capacitățile de aplicare a reglementărilor.

Concluzie

Secțiunea 4 a documentat modul în care arhitectura modulară a platformei CORB a fost realizată pentru a echilibra suveranitatea națională a datelor cu colaborarea transfrontalieră perfectă. Fiecare țară a operat o implementare complet izolată, orchestrată de Docker, care a împărtășit o singură bază de cod, dar a menținut baze de date MSSQL separate, garantând autonomia de reglementare, permițând în același timp mesageria peer-to-peer securizată între autorități.

Designul stratificat - Angular/.NET stivă front și backend, suită de micro-servicii (PAUT, RSS, notificări, raportare, mesagerie) și gazde Debian întărite - scalabil orizontal și a acceptat conducte DevSecOps. Autentificarea PAUT centralizată, MFA, acreditările Argon2hashed și canalele criptate end-to-end au protejat fiecare interacțiune, în timp ce înregistrarea în jurnal, modelele de risc controlate de versiuni și fișierele de localizare au asigurat auditabilitatea și adaptabilitatea viitoare.

Până la sfârșitul proiectului, această arhitectură a oferit o bază rezistentă și extensibilă, care a îndeplinit standardele de securitate ale ambelor țări, a facilitat coordonarea în timp real și a oferit o cale clară pentru scalarea către noi legislații, sectoare și limbi.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

SECȚIUNEA 5. CARACTERISTICI CHEIE ALE PLATFORMEI CORB

Platforma CORB oferă o gamă largă de funcții pentru entitățile operaționale și autoritățile naționale. Funcționalitatea platformei acceptă integrarea, identificarea și clasificarea end-to-end, evaluarea riscurilor, evaluarea maturității, supravegherea conformității și schimbul securizat de informații.

5.1. Integrarea și validarea entităților

- **Importul automat al datelor organizației din registrele naționale ale comerțului** (de exemplu, ONRC) prin API folosind identificatorul CUI. Suspendat până când o terță parte îndeplinește SLA-urile rezonabile.
- **Introducere și editare manuală**: Entitățile pot fi adăugate și gestionate direct în interfața platformei. Toate valorile sunt igienizate și validate în consecință. Datele adăugate sunt confirmate de utilizatorii autorității pe baza dovezilor furnizate de entitate, iar datele entității pot fi modificate oricând la cerere sau atunci când are loc o modificare.
- **Motorul de identificare și clasificare**: Entitățile sunt solicitate să răspundă la criteriile de reglementare și, în consecință, sunt desemnate în domeniul de aplicare sau în afara domeniului de aplicare al legislației NIS2. Stimularea ulterioară are ca rezultat entitățile clasificate ca esențiale, importante sau autorizate să se înregistreze ca voluntare, sprijinind alinierea NIS2.

5.2. Identificarea și evaluarea riscurilor

- **Model de risc personalizabil:** Autoritățile pot defini și actualiza regulile de evaluare a riscurilor folosind șabloane și mapări de criterii.
- **Matricea de clasificare a riscurilor:** Evaluează nivelul de risc pe baza parametrilor personalizați între actorii de risc, vectorii de atac, impactul și probabilitatea.
- **Controlul versiunilor:** Toate modelele de risc sunt dezvoltate în versiuni și marcate temporal, sprijinind urmărirea auditului și a actualizărilor.

5.3. Autoevaluarea scadenței și a conformității

- **Chestionare interactive:** Entitățile finalizează evaluări care acoperă domeniile de securitate cibernetică organizațională, operațională și tehnică.
- **Motor de punctare:** Calculează scorurile de maturitate și expunere, cu feedback vizual și rezultate exportabile.
- **Încărcarea dovezilor:** utilizatorii pot atașa documente justificative.
- **Modelul de evaluare a maturității este complet controlat și configurabil,** sprijinind alinierea la legislația în evoluție (de exemplu, NIS2, norme sectoriale precum ISO 22000 sau HACCP pentru sectorul alimentar).

5.4. Gestionarea și semnarea documentelor

- **Încărcări securizate:** Toate fișierele sunt stocate cu trasabilitate și legate de acțiunile utilizatorului.

- **Integrare semnătură electronică:** Construit pentru integrarea cu serviciile RSS pentru semnarea digitală a declarațiilor și rapoartelor. Integrarea efectivă nu este în domeniul de aplicare al acestui proiect, dar este destinată viitorului.
- **Istoricul versiunilor:** urmărește toate revizuirile și marcajele temporale ale documentelor.

5.5. Comunicare și colaborare

- **Mesagerie cu fir:** Permite comunicarea structurată între entități și autorități (de exemplu, feedback, clarificări).
- **Colaborare bazată pe sarcini:** Ofițerii pot atribui feedback sau acțiuni corective și pot bloca firul pe măsură ce este finalizat.
- **Mesagerie transfrontalieră securizată:** schimb criptat peer-to-peer de rapoarte, detalii despre incidente și coordonare între autoritățile române și bulgare.

5.6. Gestionarea utilizatorilor și a rolurilor

- **Controlul accesului bazat pe roluri (RBAC):** Management fin al permisiunilor bazat pe roluri predefinite (de exemplu, administrator de entitate, ofițer de risc).
- **Autentificare cu mai mulți factori (MFA):** Aplicată pentru toți utilizatorii, cu 2FA prin SMS sau aplicație și escaladare MFA pentru acțiunile sensibile selectate.
- **Jurnale de audit:** Toate acțiunile utilizatorilor (conectare, editări, trimiteri) sunt înregistrate pentru trasabilitate, cu marcare temporală și legătura cu identitatea unică a utilizatorului pentru a permite analiza criminalistică și raportarea de reglementare.

5.7. Monitorizare și notificări

- **Tablouri de bord de stare:** Vizualizarea progresului de integrare, scorurile de risc, postura de maturitate.
- **Alerte și notificări:** Mesaje automate pentru înregistrare, aprobări, mesaje primite pe canalul de autoritate.
- **Filtre și vizualizări personalizate:** Rapoarte ușor de personalizat pe baza tuturor datelor disponibile, filtrate după nivelul de risc, regiune sau data trimiterii.

5.8. Suport în mai multe limbi

- Complet localizat în **română, bulgară și engleză**.
- Suportă comutarea dinamică **în funcție de preferințele utilizatorului**.

5.9. Zona portalului public

- **Site web informativ:** Construit pe WordPress, oferă ghiduri de utilizare, referințe legale și întrebări frecvente.
- **Livrabile descărcabile:** Livrabilele oficiale ale proiectului sunt accesibile public alături de știri, postări de blog și alte informații relevante.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

- **Știri și anunțuri:** Întreținute de administratori pentru actualizări ale platformei și notificări de reglementare.

5.10. Export și interoperabilitate

- **Export de date:** Rezultatele sunt descărcate în format .pdf
- **Integrări API:** Pentru validarea identității (ONRC), notificări și extensii viitoare.
- **Design extensibil:** Arhitectura acceptă adăugarea de noi module sau integrări fără întreruperi de bază.

Aceste caracteristici sprijină în mod colectiv misiunea platformei CORB: să permită o cooperare eficientă, sigură și transparentă în materie de securitate cibernetică între autoritățile naționale și entitățile din sectorul alimentar.

Concluzie

Secțiunea 5 a evidențiat setul de caracteristici care a transpus planul arhitectural al CORB într-un set de instrumente complet operațional pentru entități și autorități. Integrarea automată (și manuală) a determinat domeniul de aplicare și clasificarea NIS2, în timp ce motoarele de risc și maturitate configurabile - complete cu controlul versiunilor - au oferit un scor transparent, auditabil, aliniat la legislația în evoluție. Gestionarea securizată a documentelor, pregătita pentru viitoarea integrare a semnăturilor electronice, trasabilitatea asigurată și mesageria orientată spre sarcini au permis colaborarea atât la nivel național, cât și la cea transfrontalieră.

RBAC fin cu MFA și înregistrarea exhaustivă a auditului a protejat fiecare acțiune, în timp ce tablourile de bord, alertele și interfețele multilingve au îmbunătățit conștientizarea situației și utilizarea în toate jurisdicțiile. Portalul public WordPress a diseminat îndrumări și actualizări, iar exporturile bazate pe standarde plus un strat API extensibil au pregătit platforma pentru integrare și creștere viitoare.

Împreună, aceste capabilități au echipat părțile interesate cu un mediu unic și de încredere pentru evaluarea, raportarea și coordonarea obligațiilor de securitate cibernetică în sectorul alimentar - îndeplinind misiunea platformei de cooperare eficientă, sigură și transparentă.

SECȚIUNEA 6. VALIDAREA ȘI TESTAREA PLATFORMEI

Platforma CORB a fost supusă unei campanii cuprinzătoare de validare și testare pentru a se asigura că este pregătită pentru o implementare sigură, robustă și eficientă. Faza de validare și testare a platformei a jucat un rol esențial în asigurarea faptului că platforma îndeplinește toate cerințele funcționale, de utilizare și de securitate. Testele funcționale manuale și automatizate extinse au fost efectuate de partenerii consorțiului, împreună cu o evaluare a penetrării securității în mai multe faze, pentru a verifica stabilitatea platformei, capacitatea de reacție și rezistența la amenințările cibernetice din lumea reală. Toate problemele identificate în timpul acestor procese au fost pe deplin abordate și remediate înainte de lansare.

6.1. Testarea funcțională

6.1.1. Metodologie

Testarea funcțională a urmat o abordare hibridă structurată, combinând testarea exploratorie manuală cu scripturi automate dezvoltate folosind Selenium și NUnit. Testele au vizat atât mediile desktop, cât și cele mobile, simulând comportamentul utilizatorilor administrativi, autorităților și utilizatorilor entităților în fluxuri de lucru realiste.

Procesul a inclus:

- Testarea scenariilor exploratorii
- Evaluări ale interfeței cu utilizatorul (UI/UX)
- Validarea comportamentului la nivel de componentă
- Verificarea validării intrării
- Prezentări complete ale poveștilor utilizatorului

6.1.2. Domeniu de aplicare

Testarea funcțională a acoperit toate fluxurile de lucru critice, inclusiv:

- Înregistrarea și integrarea entităților
- Logica de identificare și clasificare
- Autentificare cu mai mulți factori (MFA)
- Introducerea, editarea și validarea datelor
- Instrumente de autoevaluare a riscurilor și a maturității
- Validarea accesului bazată pe roluri și gestionarea utilizatorilor
- Mecanisme de comunicare cu autoritățile
- Tablouri de bord de susținere a deciziilor și vizualizări de raportare

6.1.3. Constatări și rezoluție

Toate **problemele** detectate au fost documentate, distribuite în **categorii de urgență critică, ridicată, medie și scăzută și programate pentru rezolvare iterativă.**

Constatările au fost legate de capacitatea de reacție, logica de filtrare și sortare, validările de câmp și suportul multilingv.

Defectele au fost remediate în ciclurile iterative de dezvoltare. Versiunea finală de lansare a rezolvat fiecare element din backlog-ul de defecte referitor la funcționalitatea critică orientată către utilizator și procesul de autoritate obișnuit și nu au rămas probleme funcționale cunoscute în acele zone.

6.2. Încercarea de penetrare

6.2.1. Domeniu de aplicare și abordare

Validarea securității a fost efectuată în 4 etape. Evaluarea a acoperit tehnicile **de cutie neagră**, **cutie gri** și **cutie albă** folosind teste manuale și automate pentru următoarele componente:

- Domeniu de aplicare
- Componenta de autentificare
- Componente backend și de infrastructură, inclusiv SSH, SSO și API-uri
- Codul sursă

Testele au simulat atacatori externi și interni cu diferite niveluri de acces și cunoștințe, acoperind:

- Top 10 vulnerabilități OWASP
- Gestionarea sesiunii și a cookie-urilor
- Robustețea MFA
- Atacuri bazate pe intrări (de exemplu, SQLi, XSS, CSRF)
- Escaladarea privilegiilor și deturnarea sesiunilor
- Exploatarea vulnerabilităților în autentificare, autorizare și gestionarea sesiunilor
- Analiza statică și dinamică a codului
- Testarea fuzz și scanarea dependențelor

6.2.2. Constatări și remediere

Vulnerabilitățile identificate în fazele inițiale și de retestare au fost clasificate și comunicate în timp real echipei de dezvoltare. Toate vulnerabilitățile critice și de mare severitate identificate în timpul testării de penetrare au fost remediate complet, retestarea confirmând atenuarea riscurilor. O rundă de retestare a confirmat eficacitatea patch-urilor și a modificărilor de configurație securizate.

Concluzie
Ciclul de viață de validare al platformei demonstrează o abordare matură și iterativă a asigurării calității și a securității cibernetice. Testarea funcțională a asigurat că toate călătoriile utilizatorilor și procesele de afaceri funcționează în mod fiabil, în timp ce două niveluri de testare de penetrare - extern și intern - au expus și corectat punctele slabe critice ale mecanismelor de autentificare și control al accesului.
După remedierea completă a tuturor constatărilor, platforma CORB este considerată stabilă, sigură și pe deplin conformă cu așteptările NIS2 și cu normele UE de securitate cibernetică.

SECȚIUNEA 7. MANUALUL

Acest capitol prezintă un manual de utilizare pas cu pas pentru testarea și interacțiunea cu platforma CORB, în special componentele de conformitate NIS2, care acționează ca o entitate. Pașii de mai jos fac parte din procesul de validare funcțională și oferă îndrumări privind simularea experienței utilizatorului final.

7.1. Pregătiți un e-mail de testare

Creați o adresă de e-mail temporară folosind platforme precum temp-mail.org sau yopmail.com. **Nu închideți fila** în care este deschisă căsuța de e-mail, deoarece veți avea nevoie de ea mai târziu pentru a prelua e-mailul de confirmare.

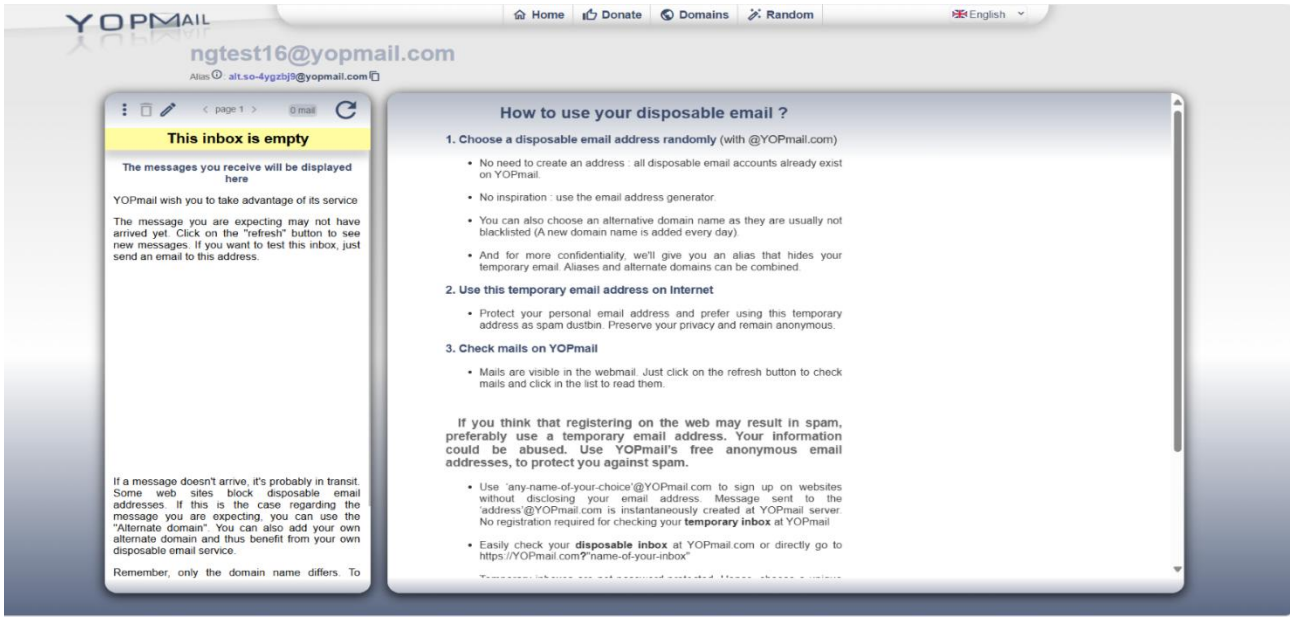

Figura 3. Platforma yopmail.com

7.2. Accesați platforma

Mergi la https://inforb.demo.certsign.ro/dashboard

> ⚠ La această adresă URL accesați mediul DEMO al platformei.

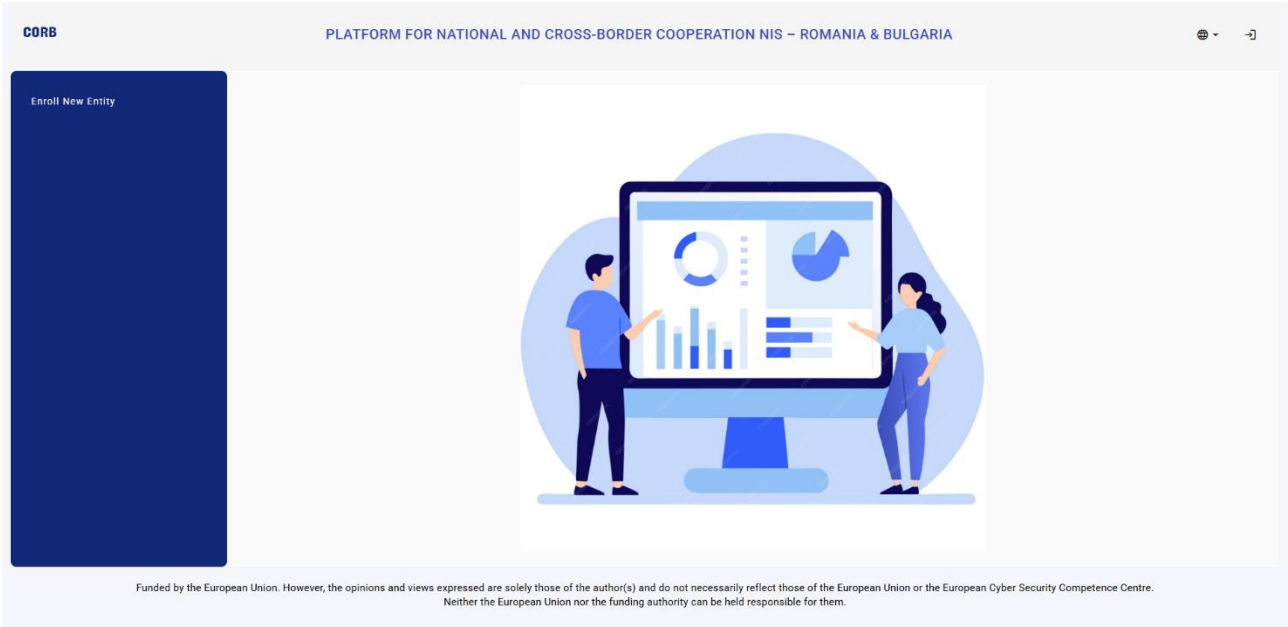

Figura 4. Prima pagină a platformei CORB

7.3. Înregistrarea unei noi entități

- Din meniul din stânga, faceți clic pe **"Înscrieți o entitate nouă".**
- Introduceți codul unic de identificare al entității dumneavoastră (CUI), apoi faceți clic pe **"Continuați"** pentru a continua.
- Completați detaliile necesare, inclusiv:
  - Adresa de e-mail de testare (creată anterior),
  - Un număr de telefon mobil valabil (de serviciu sau personal),
  - Bifați caseta de acceptare a politicii GDPR (obligatoriu).

7.4. Confirmați contul prin e-mail

- Deschideți cutia poștală temporară și așteptați câteva minute pentru e-mailul de confirmare.
- Reîmprospătați căsuța de e-mail dacă mesajul nu apare imediat.
- Faceți clic pe linkul de confirmare din e-mail pentru a continua.

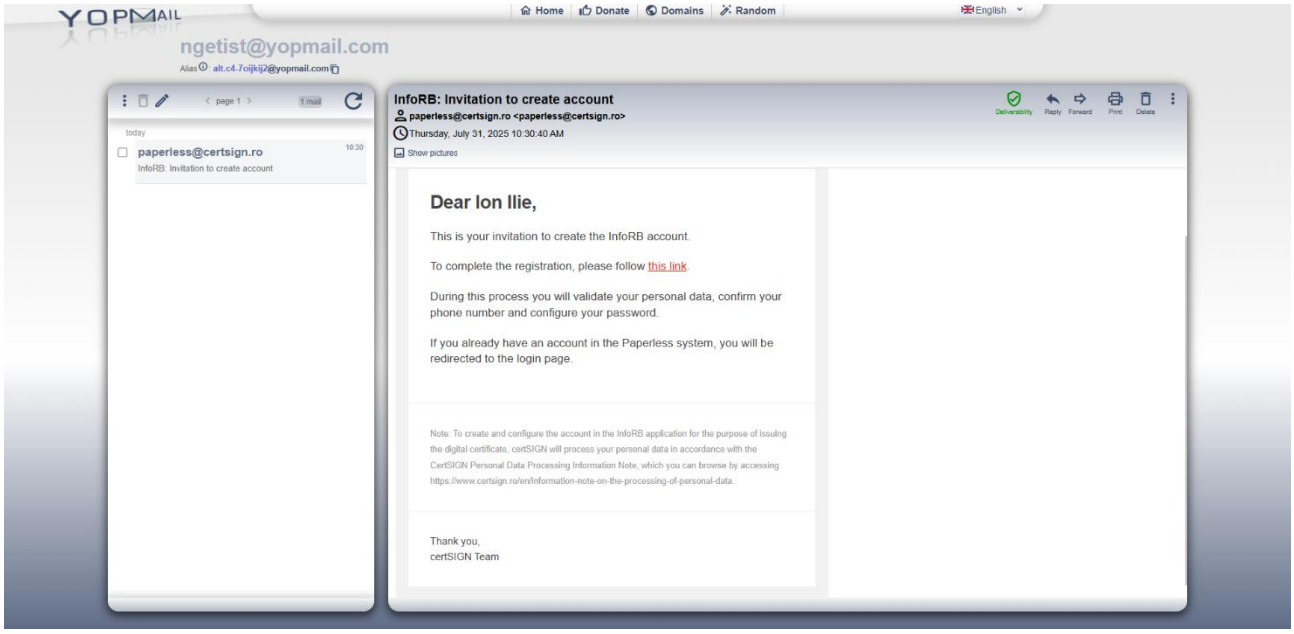

Figura 5. Yopmail.com - e-mail de confirmare

7.5. Verificarea numărului de telefon și configurarea parolei

- Veți fi redirecționat către platforma unde trebuie:
  - Confirmați-vă numărul de telefon folosind un cod SMS.

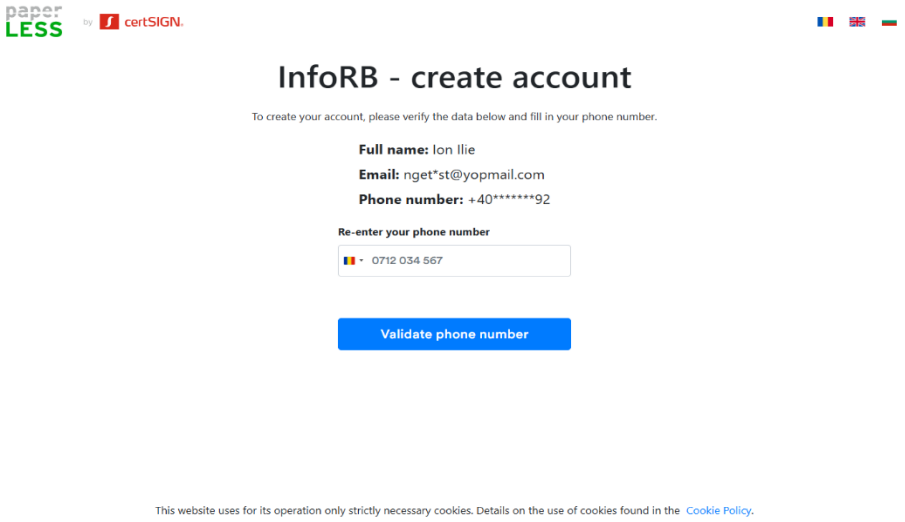

Figura 6. Verificarea numărului de telefon

  - Setați o parolă care respectă politica de complexitate a platformei.

7.6. Conectați-vă și activați MFA

- Conectați-vă folosind adresa de e-mail și parola.
- Continuați să configurați autentificarea cu mai mulți factori (2FA):
  - Instalați o aplicație de autentificare pe telefon (de exemplu, Google Authenticator).

- Scanați codul QR sau introduceți cheia de configurare.

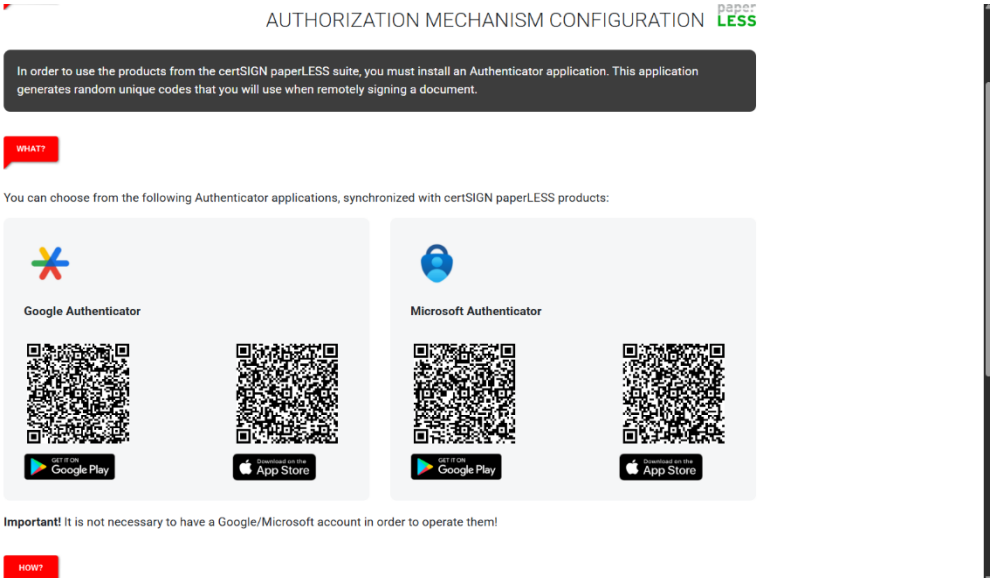

Figura 7. Configurarea mecanismului de autorizare

- Va fi trimis un al doilea SMS de verificare; Introduceți acest cod.

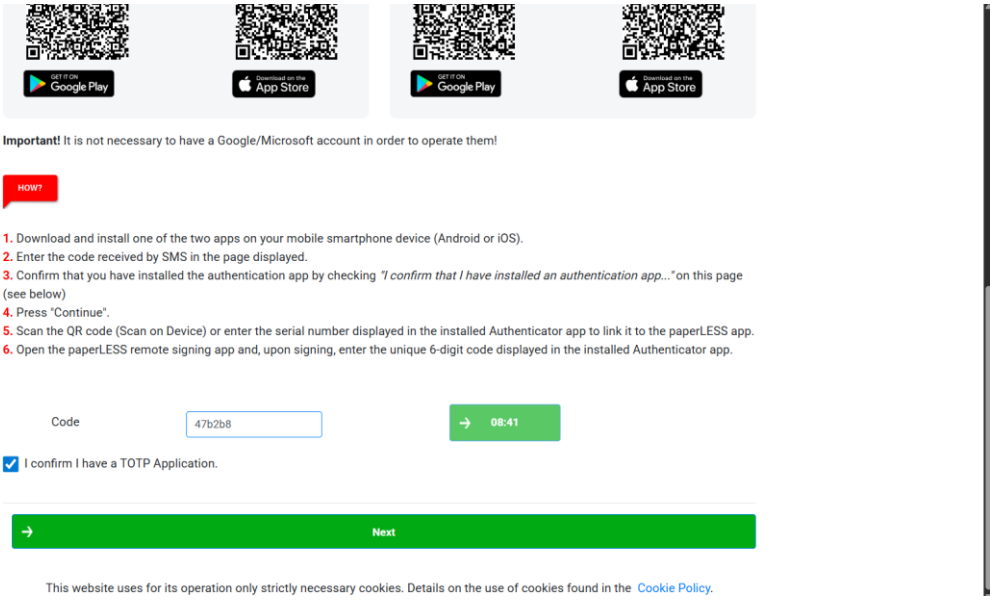

Figura 8. Aplicație de autentificare și verificare prin SMS

- Confirmați că ați instalat aplicația de autentificare bifând caseta corespunzătoare.

7.7. Integrarea completă a entității

➲ După conectarea folosind 2FA:

- Acordați acces la platformă atunci când vi se solicită.
- Din meniu, faceți clic pe **"Completați datele de înscriere".**

- Furnizați date reprezentative privind entitatea, inclusiv sectorul (de exemplu, ALIMENTE) și coduri standardizate CAEN (de exemplu, 1011 pentru „Prelucrarea cărnii”).

> ⚠ Toate câmpurile obligatorii goale vor fi marcate cu roșu.

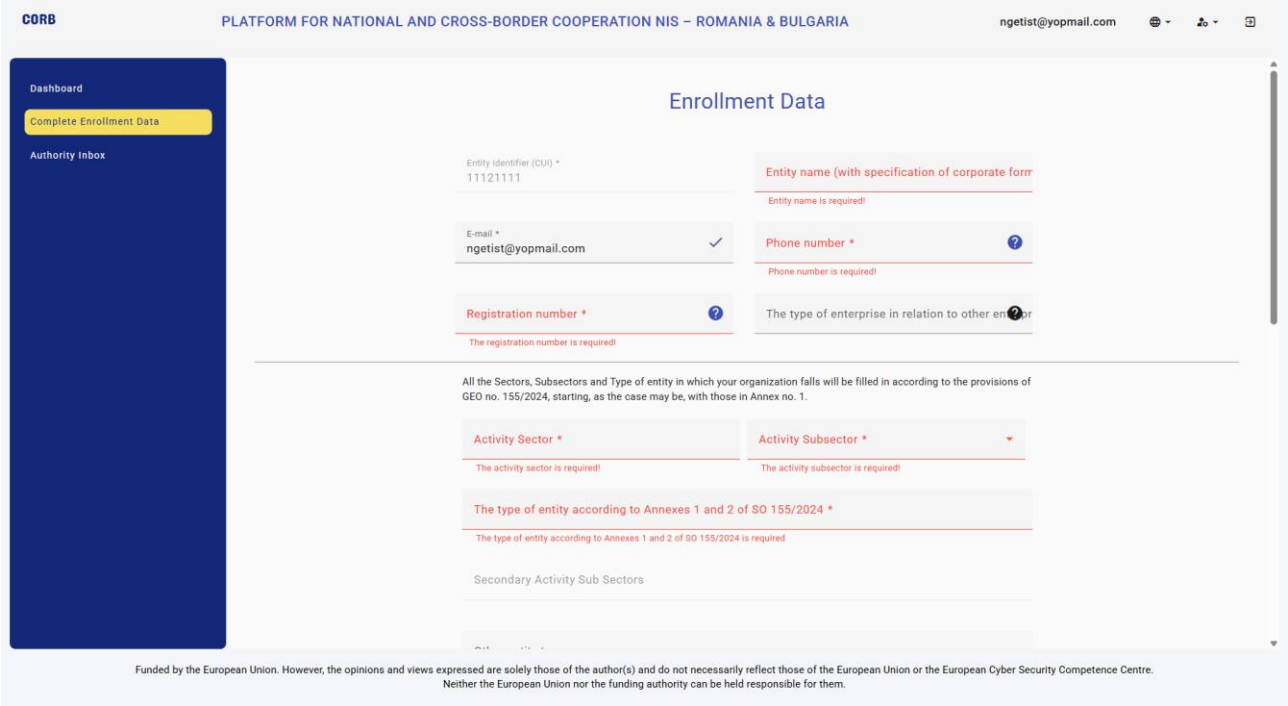

Figura 9. Depunerea datelor de înscriere.

- Faceți clic pe **"Înscrieți-vă".**

7.8. Depunerea documentelor

➲ Va fi generat un PDF pre-completat.

Figura 10. Validarea înscrierii - descărcați PDF-ul precompletat

➲ Descărcați acest PDF și **încărcați-l din nou** pe platformă, după ce îl semnați.

➲ Faceți clic pe **"Trimiteți documente".**

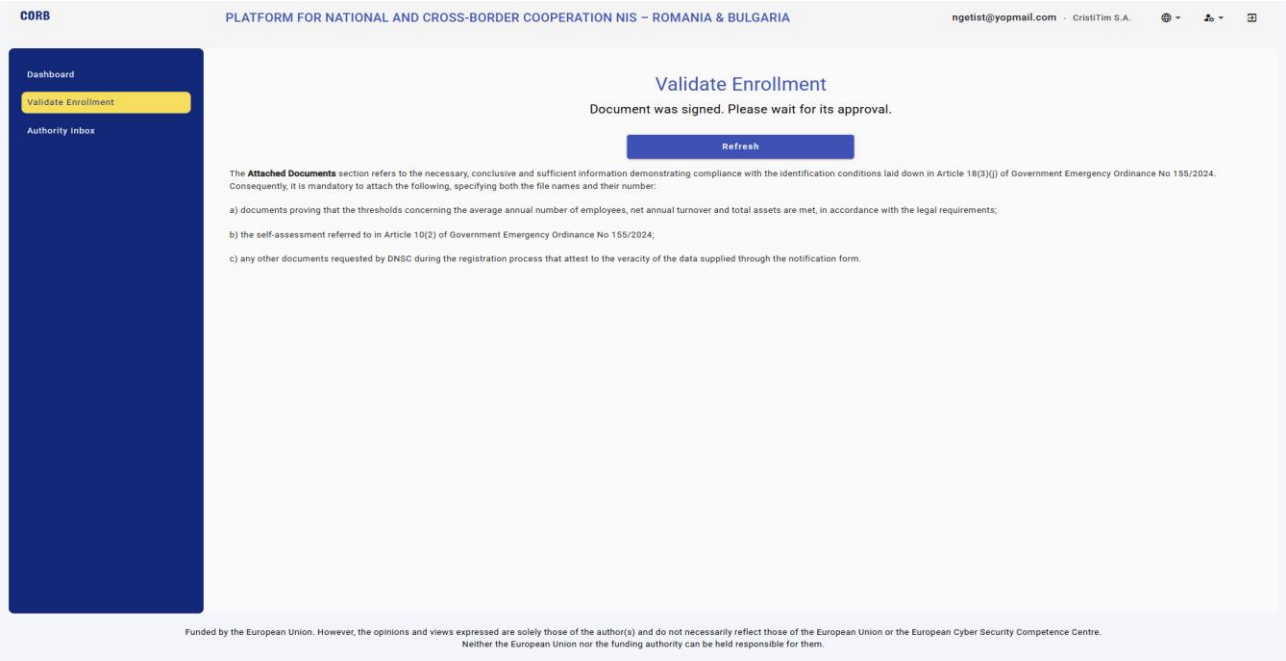

Figura 11. Validarea înscrierii - Trimiteți documentul

> ⚠ Pasul presupune: Notificarea unui administrator al Platformei CORB pentru aprobare.

7.9. Identificare și clasificare

➲ Așteptați un e-mail care anunță aprobarea:

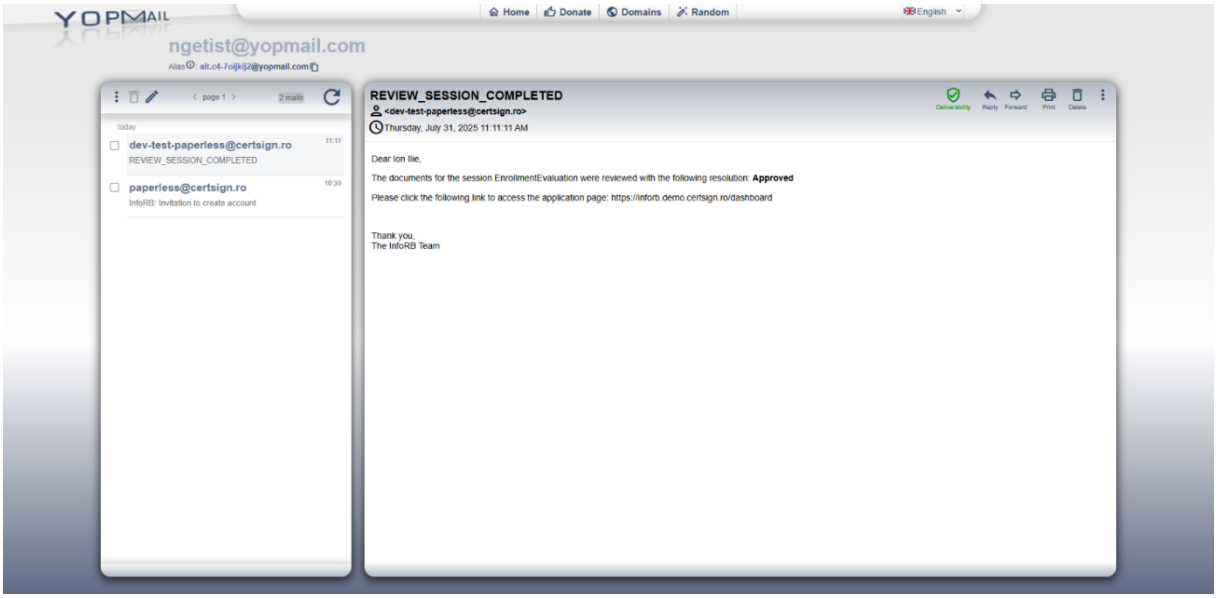

Figura 12. Evaluarea înscrierii - aprobată.

➲ După aprobare, reveniți la platformă.

- Introduceți datele de identificare și clasificare necesare și bifați casetele necesare în funcție de scenariul de testare.

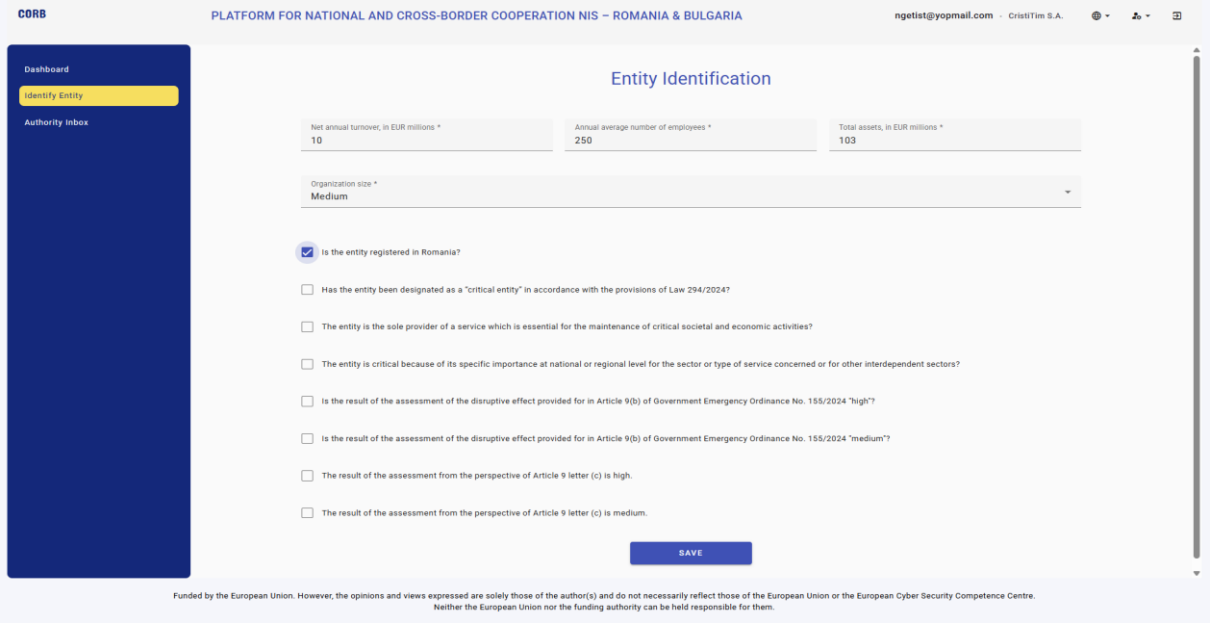

Figura 13. Identificarea entității

- Va fi generat un alt PDF care conține:
  - Toate informațiile trimise,
  - Rezultatul clasificării preliminare (esențial sau important).
- Descărcați, reîncărcați și faceți clic pe **"Trimiteți documentul".**

> ⚠ Pasul presupune: Solicitarea aprobării de către un administrator al Platformei CORB.

7.10. Evaluarea riscurilor de securitate cibernetică

- Accesați **"Evaluări ale riscurilor de securitate cibernetică".**
- Faceți clic pe **"Adăugați"** și completați câmpurile pe baza șablonului CyFun pentru sectorul relevant.

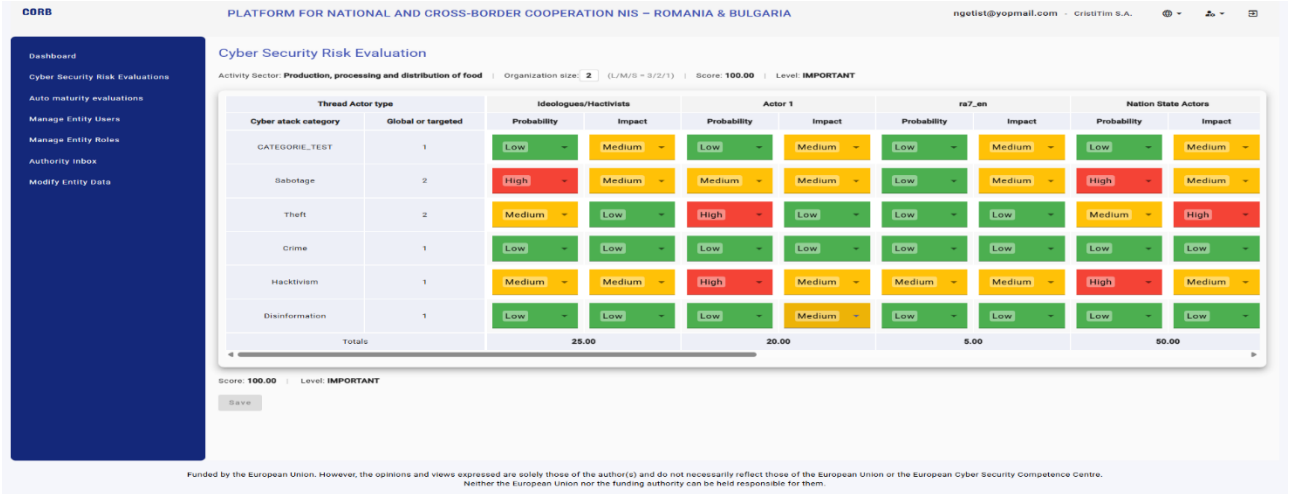

Figura 14. Evaluarea riscurilor de securitate cibernetică

➲ Salvați intrarea și încărcați fișierul PDF privind nivelul de risc generat automat (după ce a fost descărcat, asumat și semnat).

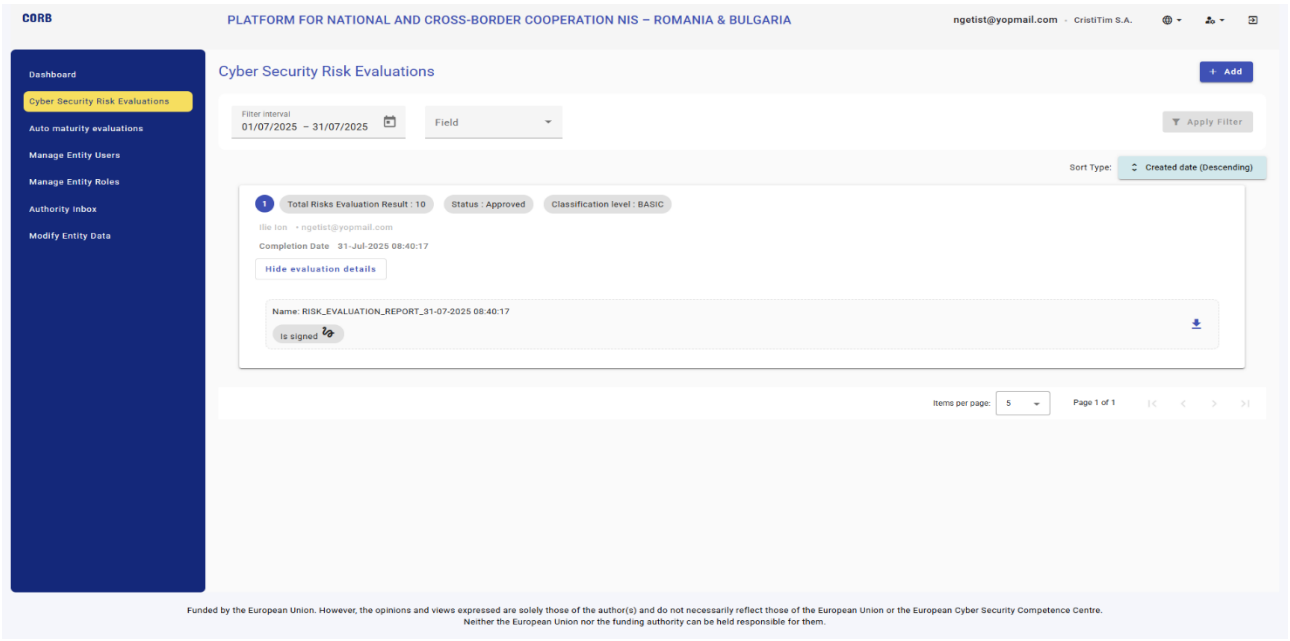

Figura 15. Rezultatul evaluării riscurilor de securitate cibernetică

⚠ Pasul presupune: Solicitarea aprobării de către un administrator al Platformei CORB.

7.11. Autoevaluarea maturității în materie de securitate cibernetică

➲ Navigați la **"Autoevaluări de maturitate".**

Figura 16. Autoevaluări ale maturității

➲ Faceți clic pe **"Adăugați",** apoi:

- Completați câmpurile de scor pentru fiecare măsură de securitate.

- Dacă scorul documentației este mai mic de 100, trebuie să completați câmpuri suplimentare, cum ar fi "Timpul documentației" și "Comentarii documentație".
- Repetați pentru scorul de implementare, dacă este cazul.

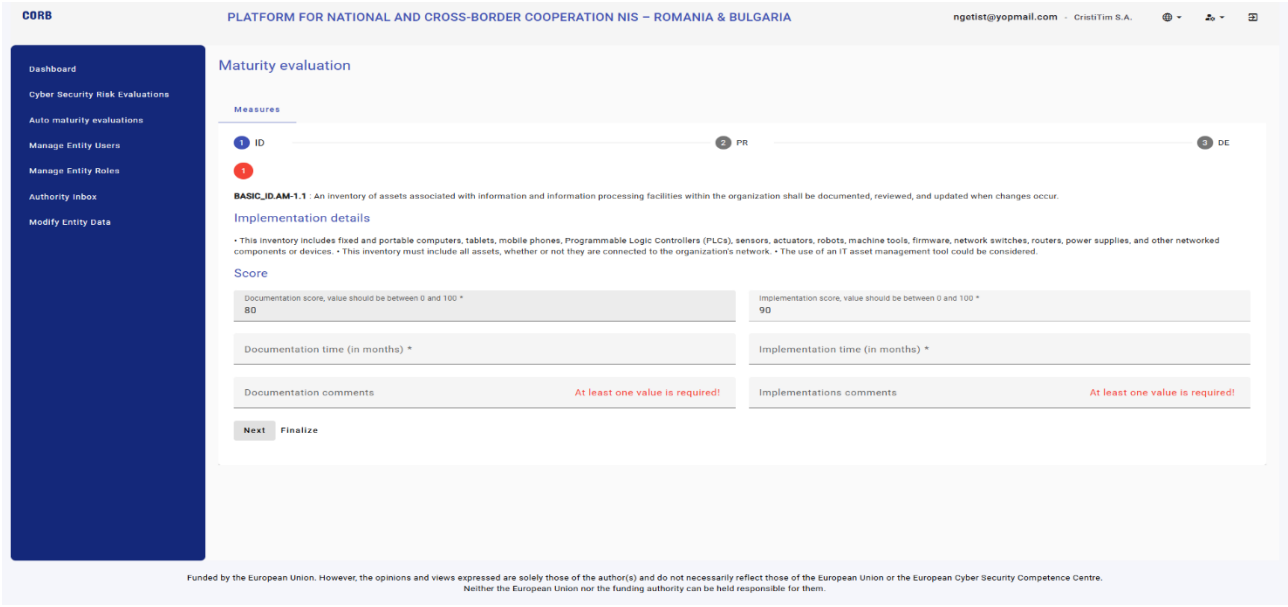

Figura 17. Evaluarea maturității - Detalii de implementare

➲ Platforma va genera un raport final de autoevaluare.

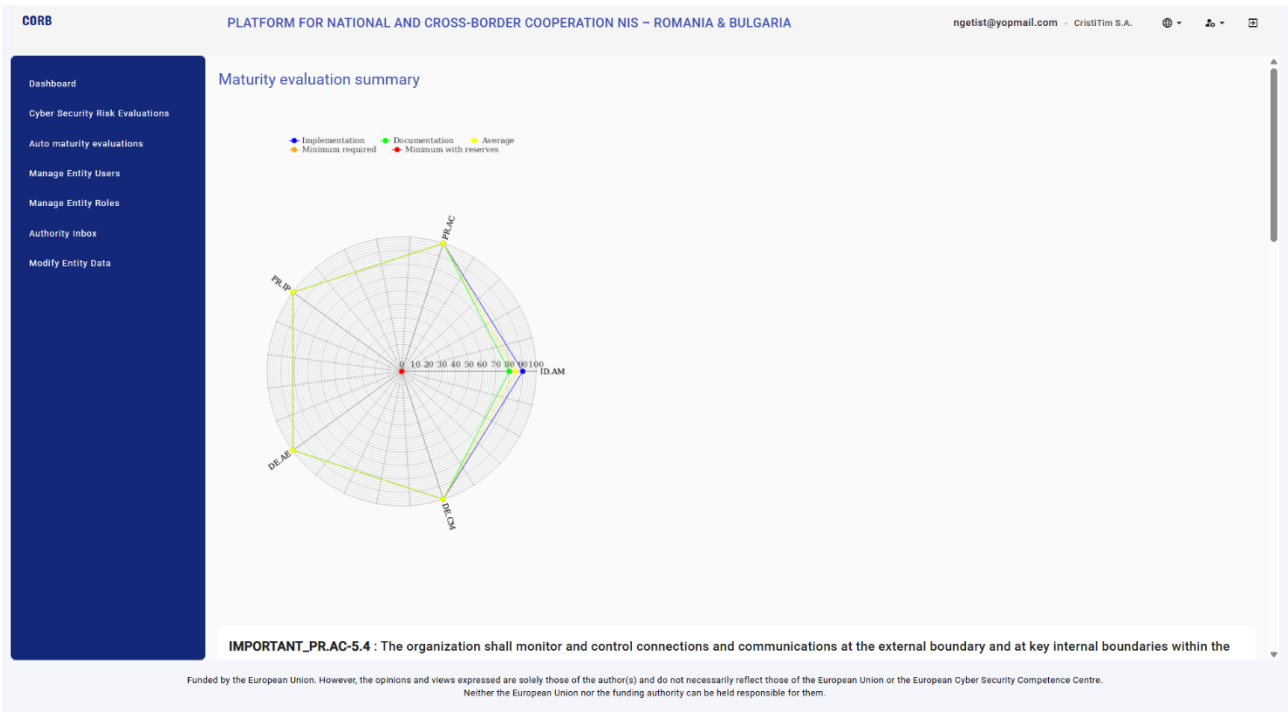

Figura 18. Rezumatul evaluării maturității

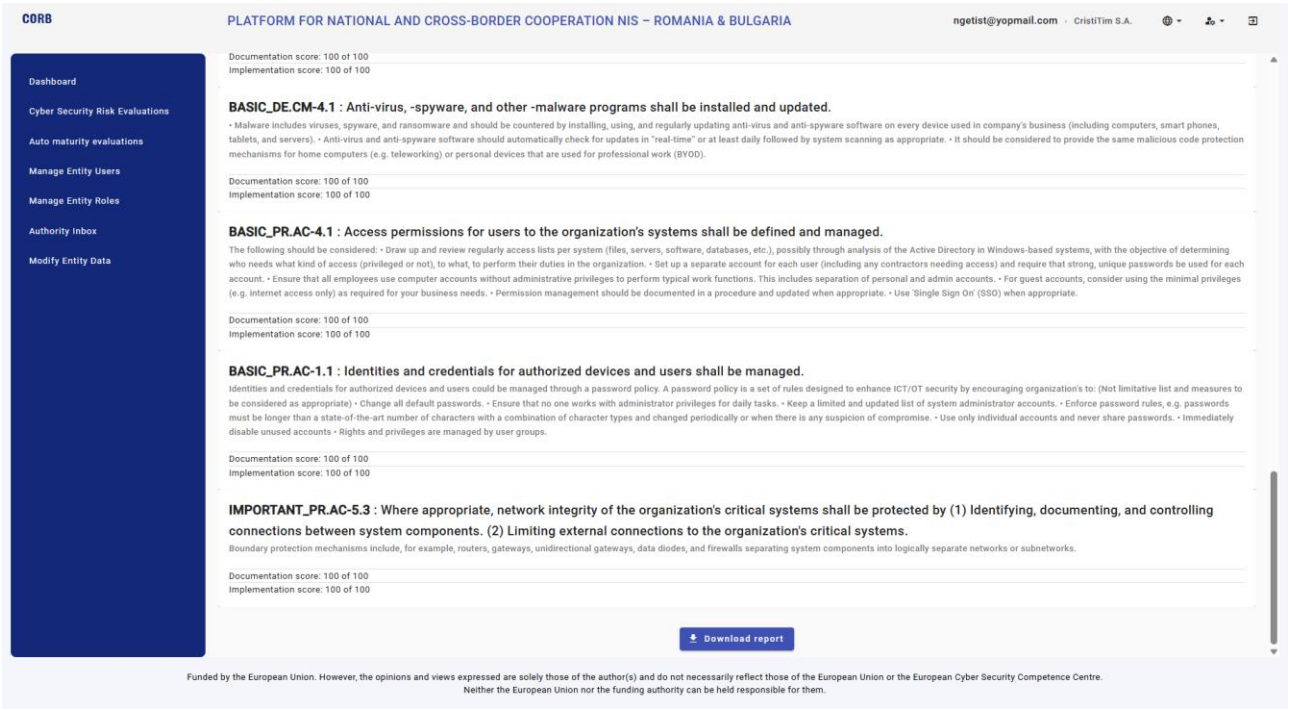

Figura 19. Raportul final de autoevaluare

➲ Descărcați raportul .PDF, reîncărcați-l și trimiteți-l pentru aprobarea (după asumare și semnare).

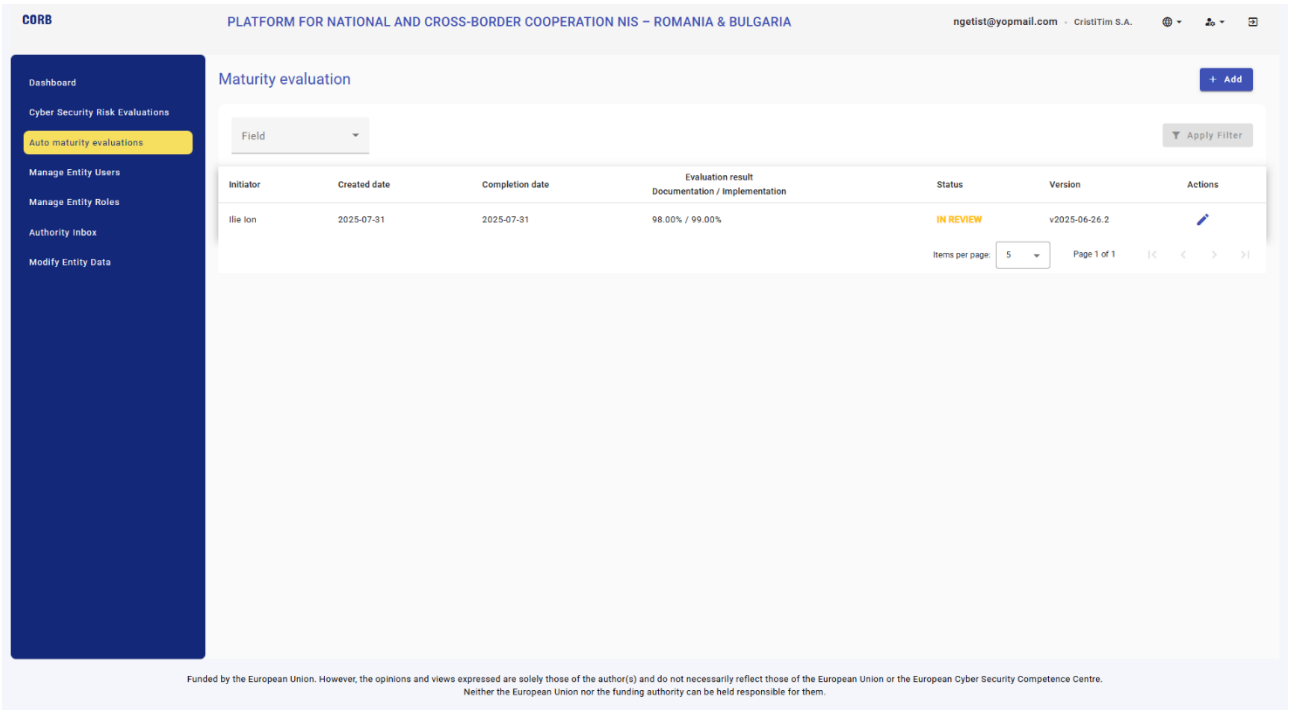

Figura 20. Autoevaluare finală / În revizuire

⚠ Pasul presupune: Solicitarea aprobării de către un administrator al Platformei CORB.

7.12 Tabloul de bord al entității

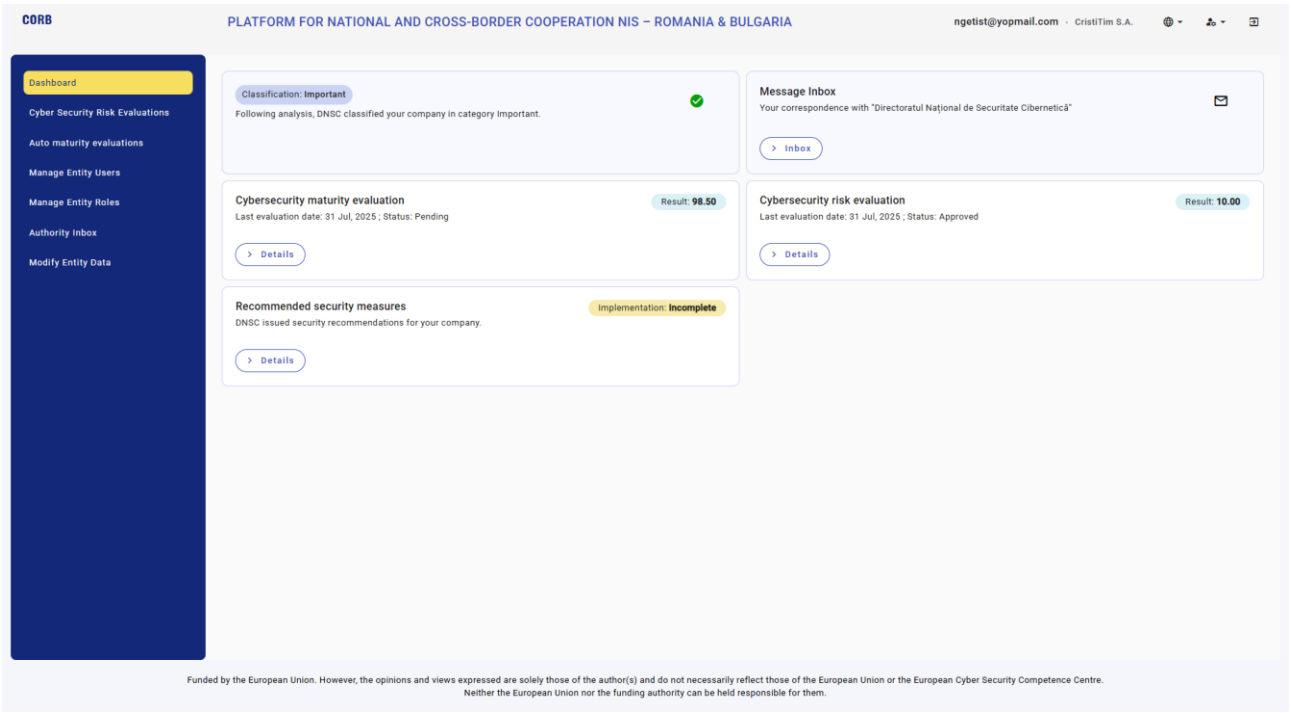

Figura 21. Tabloul de bord al entității

Tabloul de bord este doar în citire: agregă informații de stare din alte module, astfel încât să puteți identifica sarcinile restante dintr-o privire.

Insignele colorate oferă feedback instantaneu - **verde** pentru aprobat/complet, **galben** pentru articolele care mai necesită atenția dumneavoastră.

Fiecare card oferă un buton **Detalii** (sau **Inbox**) care vă duce direct la fluxul de lucru complet pentru acel element.

> ⚠ Utilizați bara de navigare din stânga pentru a vă deplasa între module fără a reveni la **tabloul de bord**.

7.13 Mesaje autoritate

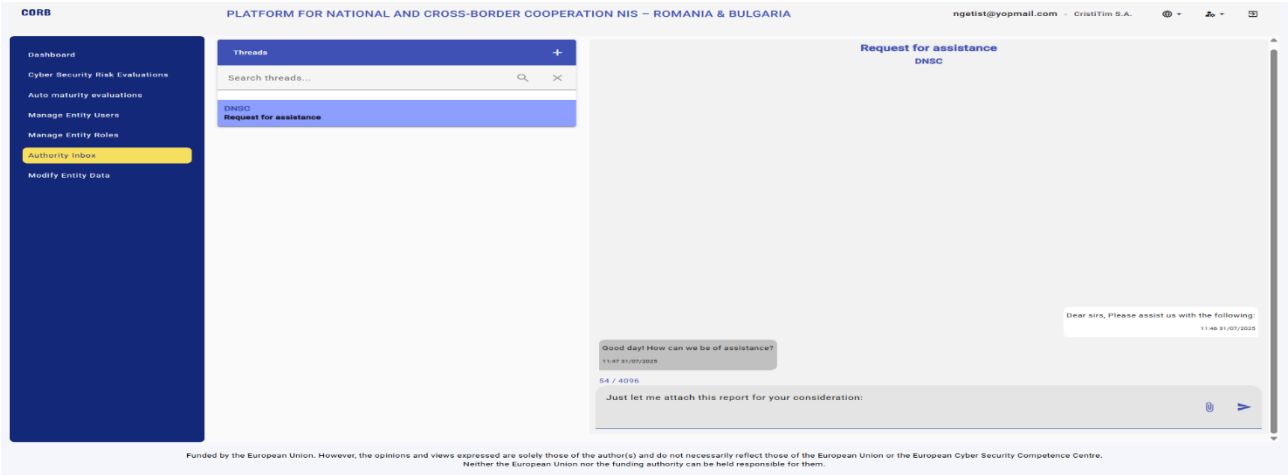

Figura 22. Autoritate - Canal de mesagerie entitate

- Pentru a trimite un mesaj nou autorității, apăsați semnul PLUS și introduceți mesajul către autoritate.
- Veți fi notificat când primește un răspuns.

7.14 Adăugarea unui utilizator nou la o entitate existentă

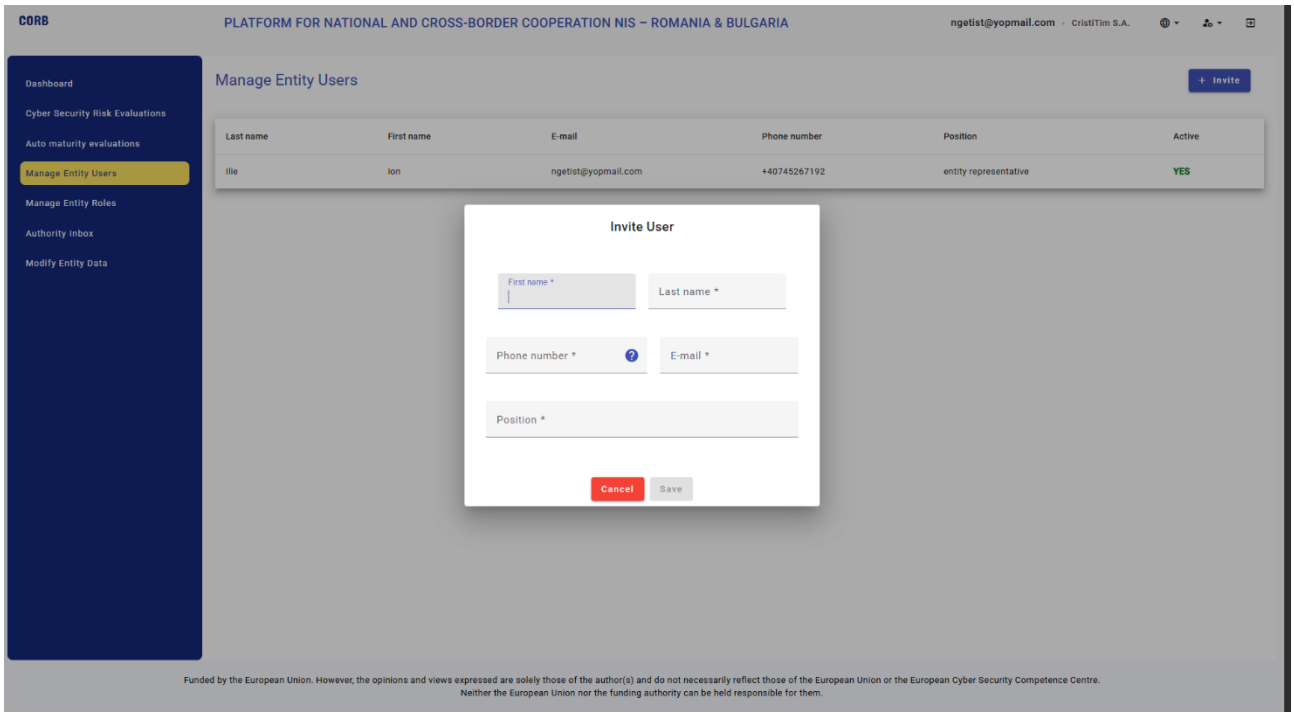

Figura 23. Adăugarea de utilizatori noi la o entitate existentă

- Pentru a adăuga un utilizator nou, introduceți datele sale de contact și apăsați Salvare.

Note suplimentare

- Toate datele de testare sunt șterse înainte ca platforma să fie lansată în producție.
- Acest proces asigură validarea amănunțită a fluxurilor de lucru de integrare, evaluare a riscurilor și autoevaluare în conformitate cu NIS2.

SECȚIUNEA 8. SECURITATE ȘI CONFIDENȚIALITATE

Securitatea și confidențialitatea datelor sunt principii fundamentale în proiectarea și operarea platformei CORB. Având în vedere natura sensibilă a datelor privind riscurile de securitate cibernetică și a informațiilor de conformitate, platforma încorporează măsuri de securitate pe mai multe niveluri pentru a asigura integritatea, confidențialitatea, disponibilitatea și responsabilitatea pentru toate datele și procesele.

8.1. Gestionarea identității și a accesului

8.1.1. Autentificare

- **Autentificare centralizată prin PAUT:** Toți utilizatorii se conectează printr-un furnizor de identitate securizat gestionat de certSIGN, care acceptă protocoalele OAuth2 și OpenID Connect.
- **Autentificare cu mai mulți factori (MFA):** obligatorie pentru toți utilizatorii, folosind tokenuri SMS sau aplicații de autentificare.
- **Aplicarea politicii de parolă**: lungimea minimă a parolei de 12 caractere, complexitatea (majuscule, mici, numerice, caractere speciale), perioada maximă de valabilitate (90 de zile) și nereutilizarea celor 5 parole anterioare, aliniate cu liniile directoare ENISA și NIST SP 800-63B.

8.1.2. Autorizare

- **Controlul accesului bazat pe roluri (RBAC):** utilizatorii au acces numai la caracteristicile și datele necesare pentru rolul lor (de exemplu, utilizator entitate, revizuitor de autorități).
- **Domeniul de aplicare specific organizației**: utilizatorii pot vizualiza sau gestiona numai înregistrările legate de organizația lor.

8.2. Confidențialitatea și izolarea datelor

- **Izolare la nivel de instanță**: România și Bulgaria operează fiecare infrastructură și baze de date separate. Datele nu sunt partajate decât dacă sunt trimise în mod explicit prin intermediul modulelor de mesagerie transfrontaliere.
- **Stocarea datelor criptate**: Datele sensibile sunt criptate în repaus folosind criptarea AES-256, cu gestionarea cheilor gestionată prin module de securitate hardware (HSM) sau soluții certificate echivalente, asigurând conformitatea cu cerințele eIDAS și GDPR.
- **Securizați datele în tranzit**: Toate comunicațiile utilizează HTTPS cu TLS 1.3 pentru a proteja împotriva interceptărilor și a atacurilor man-in-the-middle.
- **Controlul accesului la nivel de câmp**: Anumite câmpuri de înaltă sensibilitate (de exemplu, vulnerabilități specifice, evaluări) pot fi ascunse de roluri neautorizate.

8.3. Canale de comunicare securizate

- **Mesagerie criptată end-to-end**: Toate mesajele transfrontaliere între DNSC și MEGBG sunt transmise folosind protocoale peer-to-peer criptate.
- **Gestionarea sesiunii**: Expirarea automată a sesiunii și reautentificarea sunt necesare după perioade de inactivitate.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

- **Securitatea e-mailului și a notificărilor**: Serviciile de notificare sunt limitate, utilizează validarea SPF/DKIM și includ semnături digitale acolo unde este cazul.

8.4. Controale de securitate ale aplicațiilor

- **Validarea și igienizarea intrării**: Previne XSS, injecția SQL și alți vectori de atac obișnuiți.
- **Anteturi de securitate și CSP**: anteturile HTTP impuse (de exemplu, Content-Security-Policy, X-Frame-Options) atenuează atacurile bazate pe browser.
- **Înregistrarea în jurnal de audit**: Toate acțiunile utilizatorului (conectare, editări, vizualizări de date) sunt marcate și legate de identitatea utilizatorului.

8.5. Securitatea infrastructurii și a găzduirii

- **Izolarea containerelor**: Aplicația este implementată în containere Docker cu controale stricte ale resurselor și izolarea spațiului de nume.
- **Întărirea gazdei**: Serverele Debian subiacente sunt întărite conform benchmark-urilor CIS, cu servicii neutilizate dezactivate și reguli firewall.
- **Gestionarea** patch-urilor: actualizări regulate aplicate atât sistemului de operare gazdă, cât și stivei de aplicații pentru a minimiza expunerea la vulnerabilități cunoscute.
- **Integrare de detectare a intruziunilor**: Conexiune opțională la SIEM extern sau sisteme de monitorizare prin API pentru detectarea continuă a amenințărilor. DNSC implementează acest lucru, MEG BG are și această opțiune.

8.6. Integritatea și auditul datelor

- **Jurnale de audit de utilizare**: Toate acțiunile utilizatorilor din cadrul platformei sunt stocate în jurnale dedicate și pot fi revizuite de administratorii aplicației și de utilizatorii desemnați cu nivelul de acces RBAC necesar.
- **Controlul versiunii evaluărilor și modelelor de risc**: Fiecare versiune este stocată cu marcaj temporal, istoric al modificărilor și atribuire utilizatorilor.
- **Backup și recuperare**: Copii de rezervă regulate ale bazelor de date și fișierelor cu politici de retenție și proceduri testate de recuperare în caz de dezastru.

Concluzie

Secțiunea 8 a demonstrat modul în care o strategie de apărare în profunzime a protejat platforma CORB pe tot parcursul ciclului său de viață. Autentificarea PAUT centralizată, MFA obligatoriu și RBAC strict au limitat fiecare utilizator la privilegiile minime necesare, în timp ce izolarea la nivel de instanță și criptarea AES256 în repaus au păstrat suveranitatea națională a datelor și conformitatea cu GDPR. Tot traficul a circulat prin TLS 1.3, iar mascarea la nivel de câmp a restricționat și mai mult expunerea informațiilor sensibile.

Găzduirea consolidată, containerizată, gestionarea proactivă a corecțiilor și cârligele SIEM opționale au redus riscul la nivel de infrastructură, iar măsurile de protecție securizate ale codării - validarea intrărilor, anteturile CSP și înregistrarea în jurnal de audit - au protejat stratul de aplicații de exploit-urile comune. Înregistrarea continuă, controlul versiunilor și procedurile de backup testate au oferit trasabilitate completă și opțiuni de recuperare rapidă.

Împreună, aceste măsuri au asigurat îndeplinirea obiectivelor de integritate, confidențialitate, disponibilitate și responsabilitate, oferind atât autorităților române, cât și celor bulgare încredere că platforma rămâne rezistentă la amenințările cibernetice în evoluție, menținând în același timp cele mai înalte standarde de conformitate cu reglementările.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

SECȚIUNEA 9. STRATEGIA DE ÎNTREȚINERE

9.1. Întreținerea operațională

- **Actualizări programate**: Componentele de bază ale platformei, inclusiv straturile frontend, backend și baze de date, sunt actualizate în mod regulat cu patch-uri testate și îmbunătățiri ale caracteristicilor.
- **Întreținerea securității**: Se efectuează scanări regulate de vulnerabilități, verificări ale dependențelor și teste de penetrare. Patch-urile de securitate sunt aplicate în conformitate cu clasificarea severității (critic = imediat, mediu/scăzut = programat).
- **Monitorizare și timp de funcționare**: Disponibilitatea și performanța sistemului sunt monitorizate folosind instrumente la nivel de container și la nivel de gazdă. Alertele sunt generate pentru perioade de nefuncționare, servicii eșuate sau comportamente neașteptate.
- **Backup și recuperare în caz de dezastru**: Backup-urile automate regulate (incrementale și complete) sunt configurate pe instanță. Planurile de recuperare în caz de dezastru sunt testate de două ori pe an.

9.2. Asistență și asistență

- **Model de suport pe niveluri**:
  - Nivelul 1: Suport funcțional pentru navigarea platformei și problemele utilizatorilor
  - Nivelul 2: Depanare și recuperare tehnică (de exemplu, erori de formular, probleme de încărcare a documentelor)
  - Nivelul 3: Suport de dezvoltare pentru defecte de configurare sau la nivel de cod
- **Urmărirea problemelor**: Un sistem de ticketing este utilizat pentru a înregistra erori, solicitări de caracteristici și propuneri de îmbunătățire. Fiecare bilet include clasificarea severității.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

SECȚIUNEA 10. CONCLUZII ȘI CALEA DE URMAT

Dezvoltarea și implementarea platformei CORB marchează o etapă critică în consolidarea colaborării în materie de securitate cibernetică dintre România și Bulgaria, în conformitate cu Directiva NIS2. Prin construirea unui sistem sigur, modular și scalabil care acceptă atât coordonarea națională, cât și cea transfrontalieră, platforma oferă o bază solidă pentru gestionarea continuă a riscurilor, evaluarea maturității și monitorizarea conformității pentru entitățile din sectorul alimentar.

10.1. Concluzii

- Platforma sprijină cu succes **integrarea securizată**, **clasificarea riscurilor**, **autoevaluarea** și **coordonarea inter pares** între autoritățile naționale.
- **Segregarea datelor**, **accesul bazat pe roluri** și **mesageria criptată transfrontalieră** asigură conformitatea cu NIS2 și GDPR.
- Utilizarea arhitecturii moderne (Docker, .NET, Angular, MSSQL) și integrarea cu infrastructura națională (de exemplu, PAUT, RSS) s-au dovedit robuste și ușor de întreținut.

10.2. Lecții învățate

- **Nevoia de flexibilitate**: Evoluția legislației necesită șabloane extrem de configurabile, fluxuri de lucru și modele de notare care pot fi adaptate fără modificări la nivel de cod.
- **Provocări transfrontaliere**: Diferențele juridice, lingvistice și procedurale dintre țări necesită o coordonare atentă și un efort dedicat.

10.3. Planul strategic de extindere

Pentru a se alinia la întregul domeniu de aplicare al NIS2 și la peisajul amenințărilor în evoluție, platforma va fi extinsă și îmbunătățită continuu:

- Extinderea sectorială
  - **Planul pe termen scurt este de a integra toți operatorii identificați de NIS2 din toate sectoarele: energie, transporturi, finanțe, asistență medicală, infrastructură digitală, administrație publică etc.**
  - Fiecare sector nou va primi reguli personalizate de clasificare și identificare, precum și modele de risc adaptate contextului său de reglementare.
- Îmbunătățiri funcționale
  - **Fluxuri automate de informații despre amenințări** integrate direct în tablouri de bord
  - **Evaluări pre-completate și recomandări bazate pe IA** pentru colectarea de dovezi și selecția controalelor
  - **Motoare de flux de lucru** pentru automatizarea fluxului de lucru al aprobărilor autorităților
  - **Ține pasul cu cerințele legislative în evoluție**
- Angajamentul față de dezvoltarea continuă

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

Platforma CORB nu este un livrabil unic, ci un **sistem viu** care va evolua împreună cu ecosistemul de securitate cibernetică pe care îl susține. Echipa de dezvoltare și structura de guvernanță se angajează să:

- Menținerea **excelenței tehnice și a posturii de securitate a platformei.**
- Sprijinirea **utilizatorilor prin instruire și documentație.**
- Dezvoltarea platformei cu noi funcții și capabilități extinse.
- Asigurarea faptului că platforma rămâne **utilizabilă, adaptabilă și pregătită pentru viitor.**

* * *

Versiunea oficială a Documentului este în limba engleză, în timp ce la nivel național, în România și Bulgaria, va fi publicată în limbile oficiale ale acestor țări, respectiv română și bulgară.