

PLATFORM FOR NATIONAL AND CROSS-BORDER COOPERATION NIS – ROMANIA & BULGARIA [CORB].

DELIVERABLE D3.1

Version 1.0

SUMMARY

The Deliverable D3.1 “Platform for national and cross-border cooperation NIS – Romania & Bulgaria [CORB]” details the vision, requirements and high-level design of the unified cybersecurity evaluation, notification and information-sharing platform supporting Romanian and Bulgarian stakeholders in the food sector to meet the obligations of the NIS2 Directive, enabling unified cybersecurity evaluation, incident notification, and secure cross-border information exchange. It begins by mapping key actors (OES/IE, national CERTs, regulators) and their information-exchange workflows, then specifies operational, security and data-privacy requirements. It presents the platform’s modular architecture — separating national and cross-border services — and details core components (authentication, reporting dashboard, API interfaces, encryption layers). Finally, it outlines a validation plan of functional and security testing.

INFORMATION ON DOCUMENT CONTROL

Settings	Value
Title of the document:	Platform for national and cross-border cooperation NIS – Romania & Bulgaria [CORB]
Project number:	101128047
Project name:	Implementation of the NIS Directive in the food production, processing and distribution sector in Romania and Bulgaria.
Project acronym:	INFORB
Author(s) Document:	Josef KALLEDER (DNSC) Cătălin LUMEZANU, Ionut CIOBANU, Anca BOGDAN (Certsign) Viorel HORGA, Alin IACOBAN, Tiberiu BARABOI (Expertware)
Deliverable identifier:	D3.1
Delivery due date:	31.07.2025
Delivery date:	31.07.2025
Project Manager:	Constantin CĂLIN
Document version:	V1.0
Sensibility:	PU-Public
Date:	30.07.2025

Document appraisers and appraisers

Name	Role	Action	Date
Josef Kalleder	Leader of WP 3	Draft document created	15.05.2025
Josef Kalleder	Leader of WP 3	Original version (DNSC)	15.07.2025
Cătălin Lumezanu	Team Lead/Software architect/ Software Developer	Update version (CERTSIGN)	25.07.2025
Tiberiu Baraboi	Technical Advisor	Update version (EXPERTWARE)	26.07.2025
Advisory Board of Experts	Evaluation	Agreed version	30.07.2025
Constantin Călin	Project Manager	Final document agreed and delivered	31.07.2025

History of documents














Revision	Date	Created by	Brief description of the changes
V0	15.05.2025	Leader of WP 3	Document created
V0.1	15.06.2025	Leader of WP 3	Rectification of the updated document with information
V0.1.1	15.07.2025	Leader of WP 3	Updated English language
V0.1.2	25.07.2025	Team Lead/Software architect/ Software Developer	Updated English language by CERTSIGN
V0.1.3	26.07.2025	Technical Advisor	Updated English language by Bulgarian Experts
V1.0	30.07.2025	Leader of WP 3	Final document version 1

Table of contents

Information on document control.....	2
Table of Contents	3
SECTION 1. INFORB COOPERATION PLATFORM. EXECUTIVE SUMMARY	5
SECTION 2. DETAILED STRUCTURING OF ACTIVITIES	6
SECTION 3. OPERATIONAL AND TECHNICAL REQUIREMENTS	7
3.1. Operational requirements.....	7
3.1.1. Stakeholders and user roles	7
3.1.2. Core functional processes.....	7
3.1.3. Cross-border operationalization	7
3.2. Technical requirements.....	7
3.2.1. Application architecture	7
3.2.2. Authentication and authorization	8
3.2.3. Cybersecurity controls.....	8
3.2.4. Data model and integrity	8
3.2.5. Interoperability and extensibility.....	8
3.2.6. SLA and confidentiality	8
SECTION 4. SYSTEM ARCHITECTURE.....	10
4.1. High-Level Architecture Overview	10
4.2. Deployment and interconnectivity model.....	10
4.3. Data model overview	10
4.4. Communications and security architecture.....	11
4.4.1. Internal system communications	11
4.4.2. External integrations.....	11
4.5. Cross-border communication mechanism	11
4.6. Scalability and Extensibility	12
4.7. Diagram: Platform architecture (simplified).....	12
SECTION 5. KEY FEATURES OF THE CORB PLATFORM	14
5.1. Risk identification and evaluation	14
5.2. Entity onboarding & validation	14
5.3. Maturity and compliance self-assessment	14
5.4. Document management & signing	14
5.5. Communication and collaboration.....	15
5.6. User and role management	15
5.7. Monitoring and notifications	15
5.8. Multi-language support.....	15
5.9. Public portal zone	15
5.10. Export and interoperability	15
SECTION 6. PLATFORM VALIDATION AND TESTING	17

6.1. Functional testing.....	17
6.1.1. Methodology	17
6.1.2. Scope	17
6.1.3. Findings and resolution	17
6.2. Penetration testing.....	18
6.2.1. Scope and approach.....	18
6.2.2. Findings and remediation	18
SECTION 7. USER MANUAL	19
7.1. Prepare a Test Email	19
7.2. Access the platform	19
7.3. Register a new entity.....	20
7.4. Confirm account by email.....	20
7.5. Phone number verification and password setup	21
7.6. Log in and activate MFA	21
7.7. Complete entity onboarding.....	22
7.8. Document submission.....	23
7.9. Identification and classification	24
7.10. Cybersecurity risk assessment	25
7.11. Cybersecurity maturity self-assessment.....	26
SECTION 8. SECURITY AND CONFIDENTIALITY	31
8.1. Identity and access management.....	31
8.1.1. Authentication	31
8.1.2. Authorization.....	31
8.2. Data confidentiality and isolation	31
8.3. Secure communication channels.....	31
8.4. Application security controls	32
8.5. Infrastructure and hosting security	32
8.6. Data integrity and auditability	32
SECTION 9. MAINTENANCE STRATEGY	33
9.1. Operational maintenance	33
9.2. Support and helpdesk.....	33
SECTION 10. CONCLUSIONS AND WAY FORWARD.....	34
10.1. Conclusions.....	34
10.2. Lessons learned.....	34
10.3. Strategic plan for expansion	34

SECTION 1. INFORB COOPERATION PLATFORM. EXECUTIVE SUMMARY

Key	Description
Main Objective	 Design and implement a shared, scalable, cloud-native web platform that enables real-time collaboration between Romanian (DNSC) and Bulgarian (MEG-BG) cybersecurity authorities and food-sector entities, ensuring compliance with NIS2 obligations including classification, self-assessment, incident reporting, and cross-border coordination. The system supports (1) identifying and classifying essential/important entities, (2) two-way data exchange with each national authority, and (3) cross-border authority-to-authority coordination as established through the Grant Agreement.
Primary Beneficiaries	 <i>Direct:</i> <ul style="list-style-type: none"> National competent authorities (DNSC RO, MEG-BG) — enrolment entities in their respective countries, supervision of the sector & statistics. Food-sector entities (producers, processors, distributors) classed as essential or important — compliance & risk management.  <i>Indirect:</i> <ul style="list-style-type: none"> Consumers & supply-chain partners who benefit from stronger cyber resilience.
Key Functionalities	 Guided onboarding — multilingual (RO/EN/BG) flow that allows input of the company data and applies classification rules  Risk & Maturity Self-Assessments — NIS 2-mapped questionnaires with automatic scoring and history tracking  Recommendation Engine — links scores to remediation actions and cost capture  Secure Messaging & Document Hub — threaded conversations between entities and authorities, plus authority-to-authority peer channel  Dashboards & Reports — sector-wide analytics, structured data export and widgets for management & policy use  Hardened Security Core — 2FA in critical places, hashed credentials, IP/VPN-restricted admin, full user action audit logs
Expected Results	 Faster compliance — in registering food-sector entities including the completion of at least one digital self-assessment as required by law.  Cross-border insight — channel for shared RO/BG sector insights that feed EU-level situational awareness.  Knowledge diffusion — ≥ 150 public downloads of project deliverables that the public-facing module of the platform hosts  Reduced risk — measurable drop in high-severity findings across successive assessments (target ≥ 20 % reduction)

In short, the INFORB platform offers a single, secure instrument where authorities and food-sector operators can classify, assess and monitor cyber-security posture—nationally and share critical insights across the RO–BG border—delivering tangible risk reduction and streamlined NIS 2 compliance.

SECTION 2. DETAILED STRUCTURING OF ACTIVITIES

WP3		Development a platform for information and cooperation
T3.1	Development of operational requirements for the development of the CORB cooperation platform.	Defining the objectives, structure of requirements and experts. Documentation of functional and non-functional requirements, as well as performance requirements.
		Development of diagrams, sketches and interfaces necessary for the operation of the platform.
		Establish security requirements and technologies used to develop the CORB platform.
		Define and establish the cooperation between the developer and the beneficiary's representative.
		Establish the testing and validation requirements of the platform, as well as those for revision, approval, update and change management.
T3.2	Development and operationalisation 'Platform for national and cross-border cooperation NIS – Romania & Bulgaria [CORB]'.	Establishing and exposing the principles and practices used by the beneficiary and the platform developer for the delivery of a high-quality product.
		Manage and prioritise the list of platform specifications, ensure open communication in the platform development process and identify all solutions for delivering a compliant platform.
		Regular meetings between the beneficiary's representative and the CORB platform development team.
		Ensuring that a functional and testable version of the platform is delivered at the end of each sprint, as well as at the end of development.
T3.3	Testing and validation of the CORB cooperation platform.	Conduct regular tests of the platform developed to ensure the continuous quality and functionality of the software.
		Development by the developer of a test report for each sprint and release (contains: test scenarios, test results and emerging situations and will be made available through a test management system).
		Validation of tests and requesting additional test scenarios to achieve the purposes of the test. Validation for each delivered functionality of the existence of the technical documentation of the code and updating the maintenance, migration, scaling and interconnection documentation relating to that functionality and to the system as a whole.
		Validation of platform functionality and performance. Security assessment. Testing the capacity and ease of operation of the platform.

Conclusion

The activities in WP 3 established a clear route from concept to a validated CORB cooperation platform. T3.1 defined the objectives, requirements and governance rules; T3.2 converted them into working software through agile sprints with continuous beneficiary feedback; and T3.3 verified every increment through rigorous testing, security reviews and documentation checks.

Together, the three tasks formed an iterative cycle—define → develop → validate → refine—that reduced technical risk and kept the platform aligned with stakeholder needs and regulations. By the end of WP 3, the consortium delivered a production-ready, fully documented platform with a governance model that supports future change, providing a robust base for deployment, cross-border collaboration and long-term sustainability.

SECTION 3. OPERATIONAL AND TECHNICAL REQUIREMENTS

This chapter outlines the main operational and technical requirements that were drawn for the platform's successful development, deployment, and operation.

3.1. Operational requirements

3.1.1. Stakeholders and user roles

The platform serves three main user groups:

- **Entities (Essential/Important/Voluntary):** organizations designated under NIS2 as essential or important entities, or those opting for voluntary alignment with the directive.
- **Authorities (DNSC in Romania, MEGBG in Bulgaria):** responsible for oversight, risk analysis, and compliance validation.
- **Public at large:** providing information, methodologies and guidelines for the sector at large.

For the entity and authority, each user type has differentiated roles and permissions, including administrators, compliance officers, entity representatives and so on. User permissions are fine-grained, covering read/edit rights on modules such as onboarding, risk evaluation, maturity assessments, and communications.

3.1.2. Core functional processes

- **Onboarding and validation** of entities through automated (API-based) and manual data entry was implemented. However, due to the unreliability of the third-party platform that was supposed to serve us the data the platform currently relies on manual data entry, pending stabilization and SLA compliance from the third-party data provider (i.e. ONRC).
- **Entity identification and classification** was implemented using a mechanism of configurable rules and criteria. We configured such rules as needed by the current legislation, but there are mechanisms in place to make the update straightforward should the law evolve in the future.
- **Self-assessment of cybersecurity maturity and risk exposure** was implemented using customizable predefined templates grouped into versioned controlled sets. For the customization of the production version, we used the risks and maturity measures provided in the legislation currently applicable.
- **Communication workflows** between entities and authorities, including file exchange.
- **Document management** and archiving of declarations, assessments, and justifications as needed.

3.1.3. Cross-border operationalization

Each country (Romania and Bulgaria) will have its own instance of the platform, running on separate infrastructure and databases. Interoperability is ensured via peer-to-peer messaging systems for inter-authority coordination.

3.2. Technical requirements

3.2.1. Application architecture

- **Web-based, cloud-ready** application accessible via Chromium-based browsers.
- Built using **.NET Core 8.0, AngularJS 17.3.1, and NodeJS 18.**

- Hosted on **Docker containers** running **Debian 11/12**.
- Uses **MSSQL 2022** as the database engine.
- **WordPress CMS** is used for managing the public-facing informational website.

3.2.2. Authentication and authorization

- **Integrates with a central PAUT** (authentication and authorisation) **service for secure login**.
- **Enforces 2FA** (Two-Factor Authentication) **for all users**.
- **Password policies require minimum length, complexity, and periodic renewal**.
- **Implements network-level access controls**, including IP whitelisting and VPN restrictions for backend administrative endpoints.
- Implements role-based access control (RBAC) **with configurable permission schemes**.
- **All sensitive operations are logged for audit**
- **Certain critical operations require an additional MFA confirmation**.

3.2.3. Cybersecurity controls

- Passwords are stored using industry-standard cryptographic hashing algorithms such as Argon2, with salt and pepper mechanisms applied.
- Secure session management using cookies and timeout mechanisms.
- Rigorous **input sanitization** to prevent injection attacks.
- Version control for risk and maturity models to ensure auditability and regulatory compliance.

3.2.4. Data model and integrity

- Strong data typing and validation (e.g., E.123 standard for phone numbers, IBAN format validation).
- All records include traceability metadata: created_by, updated_by, timestamps.
- **Soft-delete mechanisms** ensure that data is never lost, even when logically removed from UI.

3.2.5. Interoperability and extensibility

- Interfaces with external services (ONRC) using RESTful APIs. Currently disabled due to unreliable ONRC response time.
- Imports and exports data via .csv templates for batch operations.
- Localized interface in **Romanian, English, and Bulgarian**.

3.2.6. SLA and confidentiality

- Each instance (Romania, Bulgaria) is isolated, ensuring data sovereignty.
- Access rights and data confidentiality levels are controlled per role and per organizational affiliation.
- Comprehensive audit trails are maintained for all critical operations, with tamper-evident logging mechanisms and retention policies that support post-incident forensic analysis and regulatory reporting.

Conclusion

Section 3 distilled the operational and technical prerequisites that underpinned the successful delivery of the CORB cooperation platform. Operationally, we clarified stakeholder roles, assigned fine-grained permissions, and mapped the core processes—from onboarding and maturity self-assessment to cross-border coordination—that enabled effective day-to-day use.

Technically, we defined a cloud-ready, containerized architecture built on .NET Core 8.0 and Angular 17, secured by centralized PAUT authentication, multifactor controls, and rigorous cybersecurity measures such as Argon2 password hashing and tamper-evident logging. A strict, auditable data model preserved integrity and sovereignty for the separate Romanian and Bulgarian instances, while localization, API interfaces, and clearly bounded SLAs ensured long-term extensibility and compliance.

Together, these requirements formed a detailed blueprint that steered development, minimized implementation risk, and ensured that the delivered system met both regulatory mandates and practical operational needs.

SECTION 4. SYSTEM ARCHITECTURE

The CORB Platform is architected as a modular, cloud-ready web application. Its architecture emphasizes scalability, data sovereignty, security, and interoperability.

4.1. High-Level Architecture Overview

The platform is composed of:

- **Frontend:** Web application for public users, entities, and administrators.
- **Backend (API layer):** RESTful services handling logic, authentication, and integration.
- **Microservices:**
 - Authentication & authorization (PAUT)
 - Remote Signing Service (RSS)
 - Notification engine
 - Reporting engine
 - Entity-Authority Internal Messaging Engine
- **Data layer:** MSSQL 2022 database instances, one per country instance.
- **Public zone:** WordPress CMS for informational content (static content, FAQs, methodologies, best practice guides, etc).
- **Cross-border messaging engine:** Peer-to-peer encrypted messaging between authorities.

Deployment is containerized using Docker and orchestrated using Docker Compose, hosted on hardened Debian-based systems to ensure modular scalability, fault isolation, and streamlined DevSecOps operations.

4.2. Deployment and interconnectivity model

Each country operates a **fully isolated deployment**:

Instance	Host Country	Authority	Database	Application Code
INFORB-RO	Romania	DNSC	MSSQL RO DB	Shared codebase
INFORB-BG	Bulgaria	MEGBG	MSSQL BG DB	Shared codebase

Shared codebase ensures consistency in functionality, while database stored parametrization allows for regional adjustments (catalogues, language, regulations, taxonomy).

No shared infrastructure or database exists between countries, ensuring **data sovereignty**. The systems interoperate through the secure message exchange.

4.3. Data model overview

The platform implements a relational data model designed for:

- **User and role management:** Multiple user roles using RBAC schema, MFA, activity logs.
- **Entity profiles:** Company data, food sector classification, associated persons contact data.
- **Identification and classification data:** Answers to the IDC criterias, size of the entity, no of employees, assets value and turnover.
- **Risk and maturity assessment:** Versioned questionnaires, scoring logic, justifications, recommendations.
- **Nomenclators:** Centralized lookup tables (e.g., threat actors, impact categories, security controls).
- **Catalogues** NACE codes, Country cities and towns, types of entities, etc.
- **Audit and messaging logs:** Full traceability of actions, communication threads, and document exchanges.

All core entities include:

- Unique ID
- Timestamps (created, updated)
- User metadata (created_by, updated_by)
- Soft-delete flags

4.4. Communications and security architecture

4.4.1. Internal system communications

All internal modules (frontend, backend, services) communicate using secure HTTPS and OAuth-based authentication via PAUT.

- **Session management:** Secure cookies, session timeouts
- **Data protection:** Input validation, XSS/CSRF protection, SQL injection mitigation
- **Audit logs:** tracking all user actions

4.4.2. External integrations

External System	Interface Type	Purpose
ONRC	REST API (optional)	Entity data prefill via CUI (currently suspended)
CertSIGN PAUT	OAuth / REST	User identity, 2FA, password reset
CertSIGN RSS	CSC protocol	Electronic signature (PDF uploads)
Email/SMS Gateways	SMTP/REST	Notifications and MFA delivery

4.5. Cross-border communication mechanism

To ensure real-time coordination between Romanian and Bulgarian authorities, the platform includes a **Cross-border peer messaging module**. Key features:

- **Asynchronous message queues**
- **Encrypted payloads**

- **Message routing is performed via secure gateway services that support mutual authentication, end-to-end encryption (TLS 1.3 or higher), and traceability for regulatory audit purposes.**

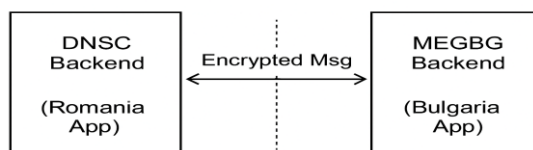


Figure 1. Diagram: Cross-border interaction.

➤ **Topic-based threading**

Each authority maintains its own logs, user sessions, and records, while selected threads and reports are shared through controlled endpoints.

4.6. Scalability and Extensibility

- **Dockerized architecture** allows modular deployment and horizontal scaling.
- **Versioned control** of risk and maturity models enables adaptation to regulatory updates.
- **Nomenclator system** supports easy extension with new sectors, rules, or scoring logic accommodating future legislation evolution.
- **Multi-language support** is integrated via localization files (RO, EN, BG).

4.7. Diagram: Platform architecture (simplified)

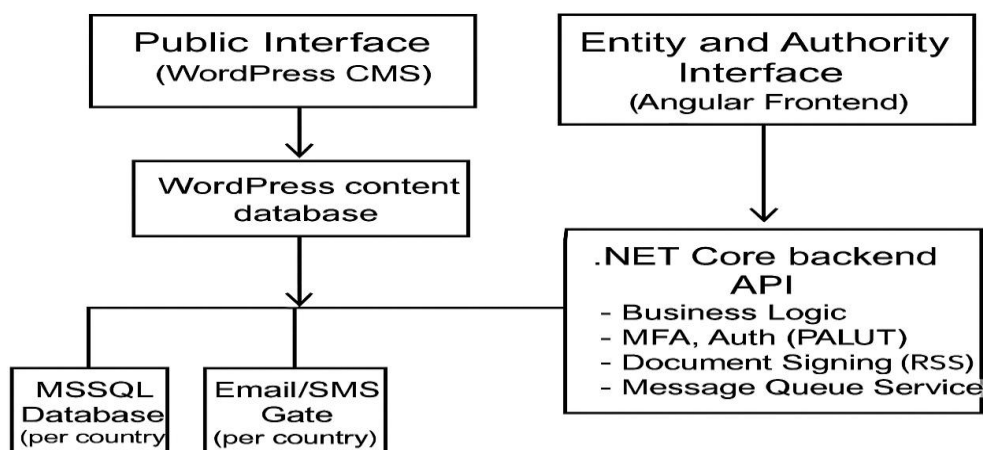


Figure 2. Diagram: Platform architecture (simplified).

This architecture ensures secure, compliant, and efficient collaboration across national borders, while preserving each country's data autonomy and regulatory enforcement capabilities.

Conclusion

Section 4 documented how the CORB Platform's modular, cloud-ready architecture was realized to balance national data sovereignty with seamless cross-border collaboration. Each country operated a fully isolated, Docker-orchestrated deployment that shared a single codebase yet maintained separate MSSQL databases, guaranteeing regulatory autonomy while enabling secure peer-to-peer messaging between authorities.

The layered design—Angular/.NET frontend-backend stack, microservice suite (PAUT, RSS, notifications, reporting, messaging), and hardened Debian hosts—scaled horizontally and supported DevSecOps pipelines. Centralized PAUT authentication, MFA, Argon2-hashed credentials, and end-to-end encrypted channels safeguarded every interaction, while tamper-evident logging, version-controlled risk models, and localization files ensured auditability and future adaptability.

By the end of the project, this architecture delivered a resilient, extensible foundation that met both countries' security standards, facilitated real-time coordination, and provided a clear pathway for scaling to new legislation, sectors, and languages.

SECTION 5. KEY FEATURES OF THE CORB PLATFORM

The CORB Platform provides a wide array of features for operational entities and national authorities. The platform's functionality supports end-to-end onboarding, identification and classification, risk evaluation, maturity assessment, compliance oversight, and secure information exchange.

5.1. Entity onboarding & validation

- **Automatic import of organization data from national business registries** (e.g., ONRC) via API using the CUI identifier. Suspended until third party meets reasonable SLAs.
- **Manual entry & editing:** Entities can be added and managed directly in the platform interface. All values are sanitized and validated accordingly. The data added is confirmed by the authority users based on the proof provided by the entity, and the entity data can always be changed upon request or when a change occurs.
- **Identification and classification engine:** Entities are prompted for answers to the regulatory criteria and accordingly are designated in scope or out of scope of the NIS2 legislation. Further prompting results in entities being classed as Essential, Important or allowed to register as Voluntary, supporting NIS2 alignment.

5.2. Risk identification and evaluation

- **Customizable risk model:** Authorities can define and update risk scoring rules using templates and criteria mappings.
- **Risk classification matrix:** Assesses risk level based on custom parameters across risk actors, attack vectors, impact and probability.
- **Version control:** All risk models are versioned and timestamped, supporting audit and update tracking.

5.3. Maturity and compliance self-assessment

- **Interactive questionnaires:** Entities complete assessments covering organizational, operational, and technical cybersecurity domains.
- **Scoring engine:** Calculates maturity and exposure scores, with visual feedback and exportable results.
- **Evidence upload:** Users can attach supporting documentation.
- **The maturity evaluation model is fully version-controlled and configurable**, supporting alignment with evolving legislation (e.g., NIS2, sectoral norms such as ISO 22000 or HACCP for food sector).

5.4. Document management & signing

- **Secure uploads:** All files are stored with traceability and linked to user actions.
- **Electronic signature integration:** Built for integration with RSS services for digitally signing declarations and reports. Actual integration is out of scope for this project but is intended for the future.

- **Version history:** Tracks all document revisions and timestamps.

5.5. Communication and collaboration

- **Threaded messaging:** Enables structured communication between entities and authorities (e.g., feedback, clarifications).
- **Task-based collaboration:** Officers can assign feedback or corrective actions and lock the thread as it is completed.
- **Secure cross-border messaging:** Peer-to-peer encrypted exchange of reports, incident details, and coordination between Romanian and Bulgarian authorities.

5.6. User and role management

- **Role-based access control (RBAC):** Fine-grained permission management based on predefined roles (e.g., entity admin, risk officer).
- **Multi-factor authentication (MFA):** Enforced for all users, with 2FA via SMS or app and MFA escalation for selected sensitive actions.
- **Audit logs:** All user actions (login, edits, submissions) are logged for traceability, with timestamping, and linkage to unique user identity to enable forensic analysis and regulatory reporting.

5.7. Monitoring and notifications

- **Status dashboards:** Visualization of onboarding progress, risk scores, maturity posture.
- **Alerts & notifications:** Automatic messages for registration, approvals, incoming messages on the authority channel.
- **Custom filters & views:** Easily customizable reports based on all available data filtered by risk level, region, or submission date.

5.8. Multi-language support

- Fully localized in **Romanian, Bulgarian, and English**.
- Supports dynamic switching **based on user preference**.

5.9. Public portal zone

- **Informational website:** Built on WordPress, provides user guides, legal references, and FAQs.
- **Downloadable deliverables:** Official project deliverables are accessible publicly alongside news, blog posts and other relevant information.
- **News and announcements:** Maintained by administrators for platform updates and regulatory notices.

5.10. Export and interoperability

- **Data export:** Results are downloaded in .pdf format

- ➔ **API integrations:** For identity validation (ONRC), notifications, and future extensions.
- ➔ **Extensible design:** Architecture supports the addition of new modules or integrations without core disruption.

These features collectively support the mission of the CORB platform: enabling efficient, secure, and transparent cooperation on cybersecurity between national authorities and food sector entities.

Conclusion

Section 5 highlighted the feature set that translated CORB's architectural blueprint into a fully operational toolset for entities and authorities. Automated (and manually fallback) onboarding determined NIS2 scope and classification, while configurable risk and maturity engines—complete with version control—provided transparent, auditable scoring aligned to evolving legislation. Secure document handling, ready for future e-signature integration, ensured traceability, and threaded, task-oriented messaging enabled both national and cross-border collaboration.

Fine-grained RBAC with MFA and exhaustive audit logging safeguarded every action, whereas dashboards, alerts, and multilingual interfaces enhanced situational awareness and usability across jurisdictions. The public WordPress portal disseminated guidance and updates, and standards-based exports plus an extensible API layer prepared the platform for integration and future growth.

Together, these capabilities equipped stakeholders with a single, trusted environment for assessing, reporting, and coordinating cybersecurity obligations in the food sector—delivering on the platform's mission of efficient, secure, and transparent cooperation.

SECTION 6. PLATFORM VALIDATION AND TESTING

The CORB platform underwent a comprehensive validation and testing campaign to ensure its readiness for secure, robust, and efficient deployment. The validation and testing phase of the platform played a critical role in ensuring the platform meets all functional, usability, and security requirements. Extensive manual and automated functional tests were conducted by consortium partners, alongside a multi-phased security penetration assessment, to verify platform stability, responsiveness, and resistance to real-world cyber threats. All identified issues during these processes were fully addressed and remediated prior to release.

6.1. Functional testing

6.1.1. Methodology

Functional testing followed a structured hybrid approach, combining manual exploratory testing with automated scripts developed using Selenium and NUnit. The tests targeted both desktop and mobile environments, simulating the behaviour of administrative users, authorities, and entity users across realistic workflows.

The process included:

- Exploratory scenario testing
- User Interface (UI/UX) assessments
- Component-level behavior validation
- Input validation verification
- End-to-end user story walkthroughs

6.1.2. Scope

Functional testing covered all mission-critical workflows, including:

- Entity registration and onboarding
- Identification and Classification logic
- Multi-factor authentication (MFA)
- Data input, editing, and validations
- Risk and maturity self-assessment tools
- Role based access validation and user management
- Communication mechanisms with authorities
- Decision supporting dashboards and reporting views

6.1.3. Findings and resolution

All detected **issues** were documented, distributed into **Critical, High, Medium and Low categories of urgency and scheduled for iterative resolving**.

Findings were related to responsiveness, filtering and sorting logic, field validations, and multilingual support.

Defects were remediated in iterative development cycles. The final release version resolved every item in the defect backlog pertaining to critical user-facing functionality and regular authority process, and no known functional issues remain in those areas.

6.2. Penetration testing

6.2.1. Scope and approach

The security validation was carried out in 4 stages. The assessment covered **black-box**, **gray-box**, and **white-box** techniques using manual and automated tests for the following components:

- Application domain
- Authentication component
- Backend and infrastructure components including SSH, SSO, and APIs
- Source code

The tests simulated external and internal attackers with varying levels of access and knowledge, covering:

- OWASP Top 10 vulnerabilities
- Session and cookie handling
- MFA robustness
- Input-based attacks (e.g., SQLi, XSS, CSRF)
- Privilege escalation and session hijacking
- Vulnerability exploitation in authentication, authorization, and session management
- Static and dynamic code analysis
- Fuzz testing and dependency scanning

6.2.2. Findings and remediation

Vulnerabilities identified during initial and retest phases were categorized and communicated in real-time to the development team. All critical and high-severity vulnerabilities identified during penetration testing were fully remediated, with retesting confirming risk mitigation. A retesting round confirmed the effectiveness of the patches and secure configuration changes.

Conclusion

The platform's validation lifecycle demonstrates a mature and iterative approach to quality assurance and cybersecurity. Functional testing ensured all user journeys and business processes operate reliably, while two layers of penetration testing—external and internal—exposed and corrected critical weaknesses in authentication and access control mechanisms.

Following the complete remediation of all findings, the CORB platform is deemed stable, secure, and fully compliant with NIS2 expectations and EU cybersecurity norms.

SECTION 7. USER MANUAL

This chapter presents a step-by-step user manual for testing and interacting with the CORB platform, particularly the NIS2 compliance components, acting as an entity. The steps below are part of the functional validation process and provide guidance on simulating the end-user experience.

7.1. Prepare a Test Email

Create a temporary email address using platforms such as temp-mail.org or yopmail.com. **Do not close the tab** where the inbox is open, as you will need it later to retrieve the confirmation email.

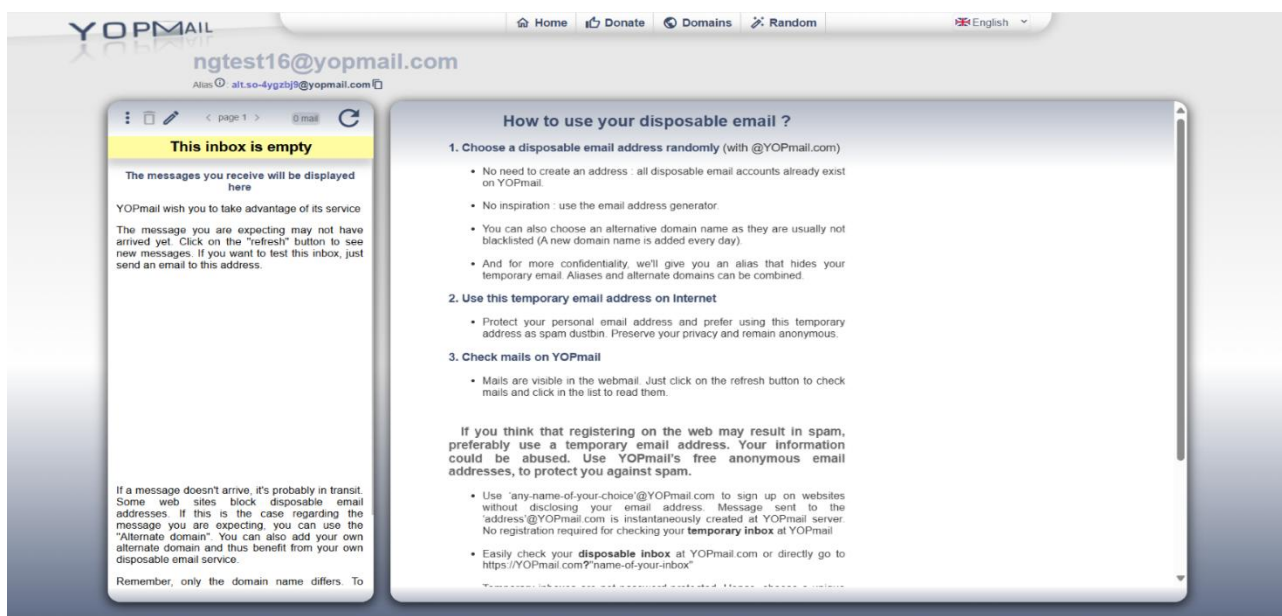


Figure 3. Platform yopmail.com

7.2. Access the platform

Go to <https://inforb.demo.certsign.ro/dashboard>

⚠ At this URL you are accessing the DEMO environment of the platform.

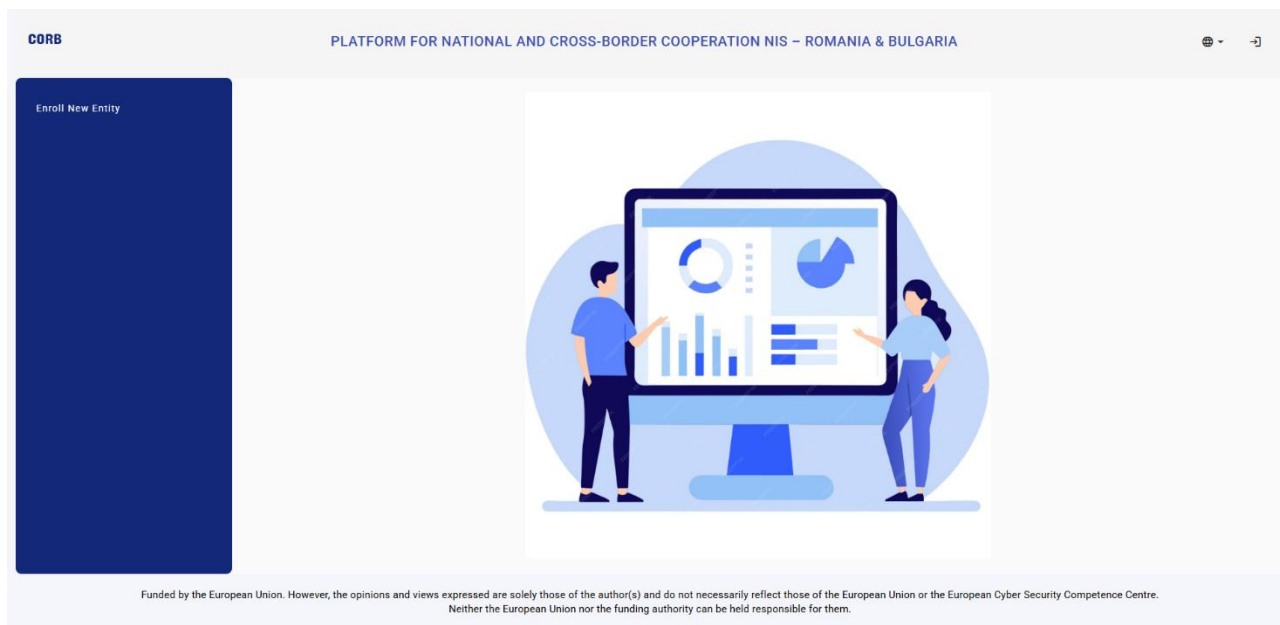


Figure 4. Front page of the CORB platform

7.3. Register a new entity

- ➔ From the left-hand menu, click on **“Enrol New Entity”**.
- ➔ Enter the company’s unique identifier (CUI), then click **“Continue”** to proceed.
- ➔ Fill in the required details, including:
 - Your test email address (created previously),
 - A valid mobile phone number (work or personal),
 - Check the GDPR policy acceptance box (mandatory).

7.4. Confirm account by email

- ➔ Open your temporary mailbox and wait a few minutes for the confirmation email.
- ➔ Refresh the inbox if the message does not appear immediately.
- ➔ Click on the confirmation link in the email to proceed.

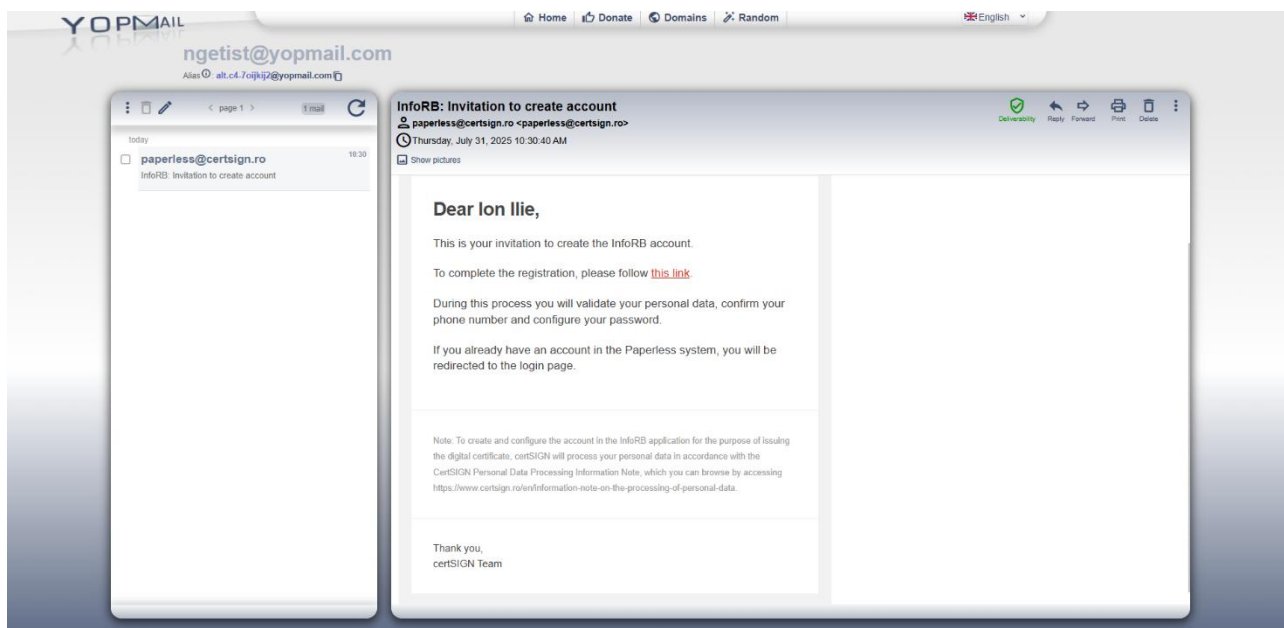


Figure 5. Yopmail.com - confirmation email

7.5. Phone number verification and password setup

- ➔ You will be redirected to the platform where you must:
 - Confirm your phone number using an SMS code.



InfoRB - create account

To create your account, please verify the data below and fill in your phone number.

Full name: Ion Ilie
Email: nget*st@yopmail.com
Phone number: +40*****92

Re-enter your phone number

🇷🇴 0712 034 567

Validate phone number

This website uses for its operation only strictly necessary cookies. Details on the use of cookies found in the [Cookie Policy](#).

Figure 6. Verification of phone number

- Set a password that complies with the platform's complexity policy.

7.6. Log in and activate MFA

- ➔ Log in using your email and password.
- ➔ Proceed to configure Multi-Factor Authentication (2FA):
 - Install an authenticator app on your phone (e.g., Google Authenticator).

- Scan the QR code or enter the setup key.

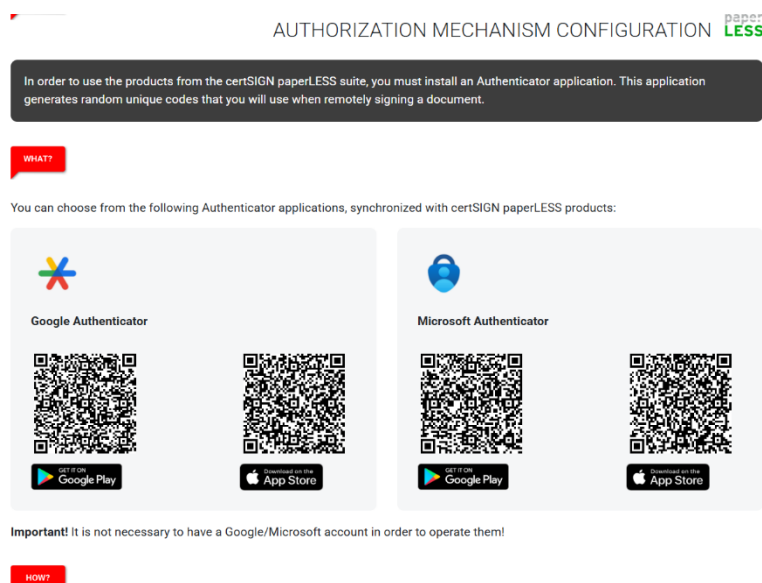


Figure 7. Authorization mechanism configuration

- A second verification SMS will be sent; enter this code.

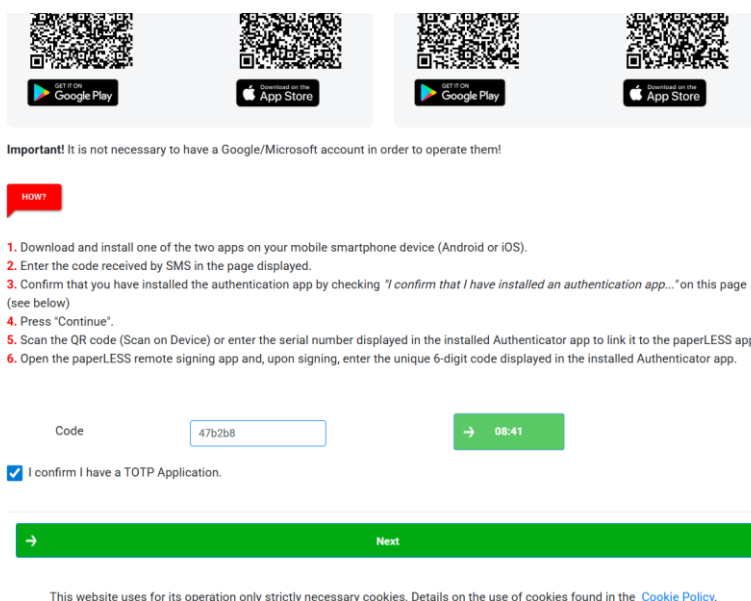


Figure 8. Authenticator app and SMS verification

- Confirm you have installed the authenticator app by ticking the corresponding box.

7.7. Complete entity onboarding

➡ After logging in using 2FA:

- Grant platform access when prompted.
- From the menu, click “Complete enrolment data”.

- Provide representative company data including sector (i.e. FOOD) and standardized NACE codes (e.g., 1011 for meat processing).
 - All empty required fields will be marked red.

CORB PLATFORM FOR NATIONAL AND CROSS-BORDER COOPERATION NIS – ROMANIA & BULGARIA ngetist@yopmail.com

Enrollment Data

Entity Identifier (CUI) *
11121111

Entity name (with specification of corporate form)
Entity name is required!

E-mail *
ngetist@yopmail.com ✓

Phone number *
Phone number is required!

Registration number *
The registration number is required!

The type of enterprise in relation to other enterprises *

All the Sectors, Subsectors and Type of entity in which your organization falls will be filled in according to the provisions of GEO no. 155/2024, starting, as the case may be, with those in Annex no. 1.

Activity Sector *
The activity sector is required!

Activity Subsector *
The activity subsector is required!

The type of entity according to Annexes 1 and 2 of SO 155/2024 *
The type of entity according to Annexes 1 and 2 of SO 155/2024 is required

Secondary Activity Sub Sectors

Funded by the European Union. However, the opinions and views expressed are solely those of the author(s) and do not necessarily reflect those of the European Union or the European Cyber Security Competence Centre. Neither the European Union nor the funding authority can be held responsible for them.

Figure 9. Enrolment data submission.

- Click “Enrol”.

7.8. Document submission

- ➡ A pre-filled PDF will be generated.

CORB PLATFORM FOR NATIONAL AND CROSS-BORDER COOPERATION NIS – ROMANIA & BULGARIA ngetist@yopmail.com - Cristin S.A.

Validate Enrollment

Download Representative Document

Upload Signed Document

Upload Justifying Documents

Submit documents

Secțiunea **Documente anexate** se referă la informațiile necesare, concludente și suficiente din care să rezulte îndeplinirea condițiilor pentru identificare conform dispozițiilor art. 10 alin. (3) lit. j) din Ordonanța de urgență a Guvernului nr. 155/2024, fiind astfel obligatorie atestarea următoarelor, cu precizarea denumirilor fișierelor atașate, cât și a numărului acestora:

a) documentele care atestă încadrarea în platanele referitoare la numărul mediu anual de salariați, cifra de afaceri anuală netă și activele totale, conform cerințelor legale;

b) autoevaluarea conform ordinului prevăzut la art. 10 alin.(2) din Ordonanța de urgență a Guvernului nr. 155/2024;

c) alte documente solicitate de către DNSC, în cadrul procesului de înregistrare, care atestă veridicitatea datelor furnizate prin intermediul formularului de notificare.

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 funding authority can be held responsible for them.

Figure 10. Enrolment validation - download pre-filled PDF

- ➡ Download this PDF and **re-upload it** to the platform.

➔ Click “Submit Documents”.

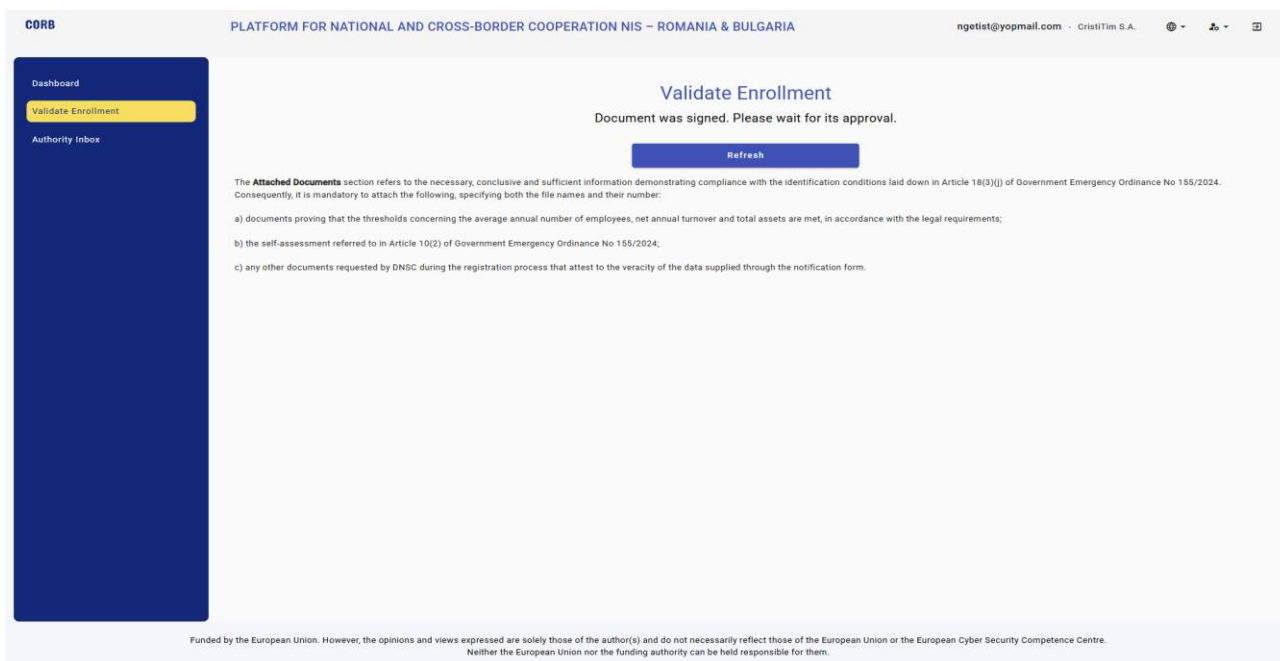


Figure 11. Enrolment validation - Submit Document

➔ Notify one of the platform administrators (Josef KALLEDER) for approval.

7.9. Identification and classification

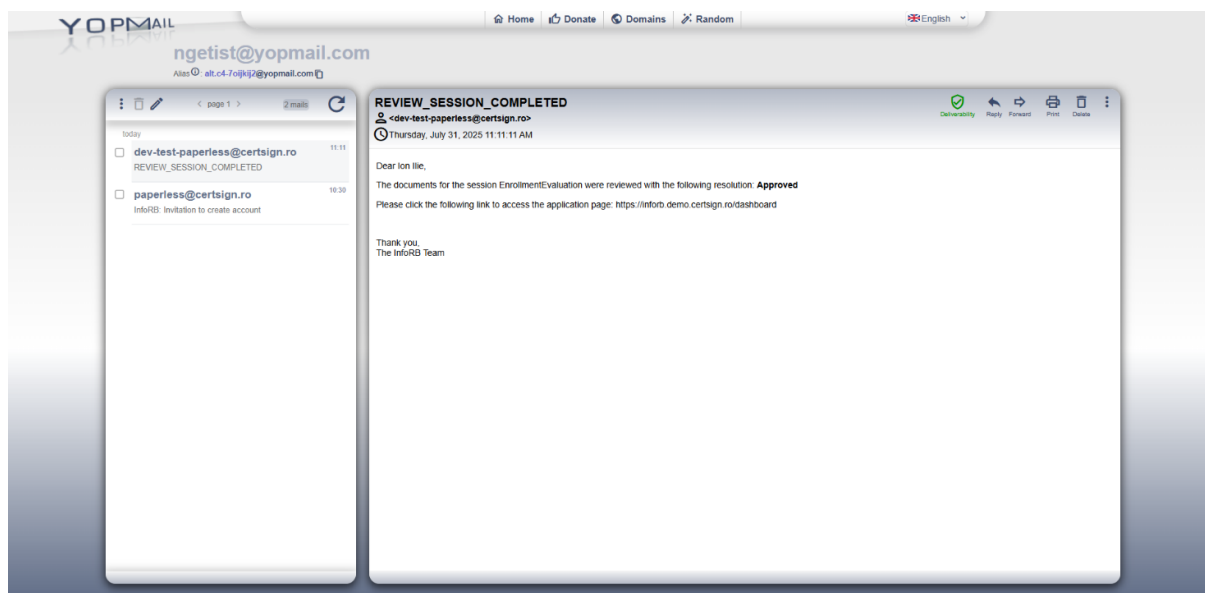


Figure 12. Enrolment Evaluation - approved.

- ➔ Wait for an email announcing the approval:
- ➔ Once approved, return to the platform.

- ➔ Enter the required identification and classification data and tick the necessary boxes based on the test scenario.

The screenshot shows the 'Entity Identification' form in the CORB platform. The form includes fields for 'Net annual turnover, in EUR millions *' (10), 'Annual average number of employees *' (250), and 'Total assets, in EUR millions *' (103). A dropdown menu for 'Organization size *' is set to 'Medium'. Below these are several checkboxes for entity registration and criticality assessments. The 'Is the entity registered in Romania?' checkbox is checked. A 'SAVE' button is at the bottom right.

Figure 13. Identifying the entity

- ➔ Another PDF will be generated containing:
 - All submitted information,
 - The preliminary classification result (Essential or Important).
- ➔ Download, re-upload, and click “**Submit Document**”.
- ➔ Request document approval from an administrator.

7.10. Cybersecurity risk assessment

- ➔ Go to “**Cybersecurity Risk Evaluations**”.
- ➔ Click “**Add**”, and fill in the fields based on the CyFun template for the relevant sector.

The screenshot shows the 'Cyber Security Risk Evaluation' form. It includes a table for 'Cyber stack category' and 'Global or targeted' with rows for 'Sabotage', 'Theft', 'Crime', 'Hacktivism', and 'Disinformation'. Below the table is a 'Totals' row. The form also includes a 'Score' field (100.00) and a 'Level' field (IMPORTANT). A 'Save' button is at the bottom left.

Figure 14. Cyber security risk assessment

- Save your entry and upload the automatically generated risk level PDF from your Downloads folder.

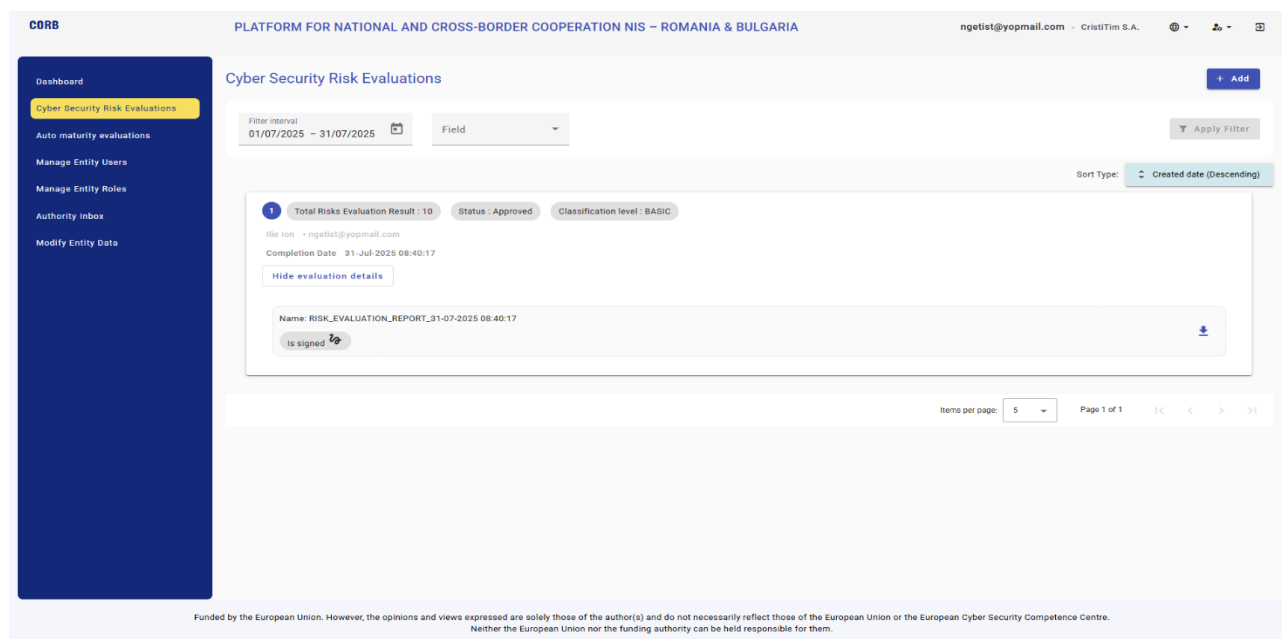


Figure 15. Outcome of the cyber security risk assessment

Figure 15. Outcome of the cyber security risk assessment

- Request approval from an administrator.

7.11. Cybersecurity maturity self-assessment

- Navigate to “Maturity Self-Assessments”.



Figure 16. Maturity self-assessments

Figure 16. Maturity self-assessments

➡ Click “Add”, then:

- Complete the score fields for each security measure.
- If the documentation score is less than 100, you must complete additional fields such as “Documentation Time” and “Documentation Comments.”
- Repeat for implementation score if applicable.

Measure

1 ID 2 PR 3 DE

BASIC_ID.AM-1.1 : An inventory of assets associated with information and information processing facilities within the organization shall be documented, reviewed, and updated when changes occur.

Implementation details

• This inventory includes fixed and portable computers, tablets, mobile phones, Programmable Logic Controllers (PLCs), sensors, actuators, robots, machine tools, firmware, network switches, routers, power supplies, and other networked components or devices. • This inventory must include all assets, whether or not they are connected to the organization's network. • The use of an IT asset management tool could be considered.

Score

Documentation score, value should be between 0 and 100 *	Implementation score, value should be between 0 and 100 *
80	90

Documentation time (in months) *	Implementation time (in months) *

Documentation comments	Implementations comments
At least one value is required!	At least one value is required!

Next Finalize

Funded by the European Union. However, the opinions and views expressed are solely those of the author(s) and do not necessarily reflect those of the European Union or the European Cyber Security Competence Centre. Neither the European Union nor the funding authority can be held responsible for them.

Figure 17. Maturity assessment - Implementation details

➡ The platform will generate a final self-assessment report.

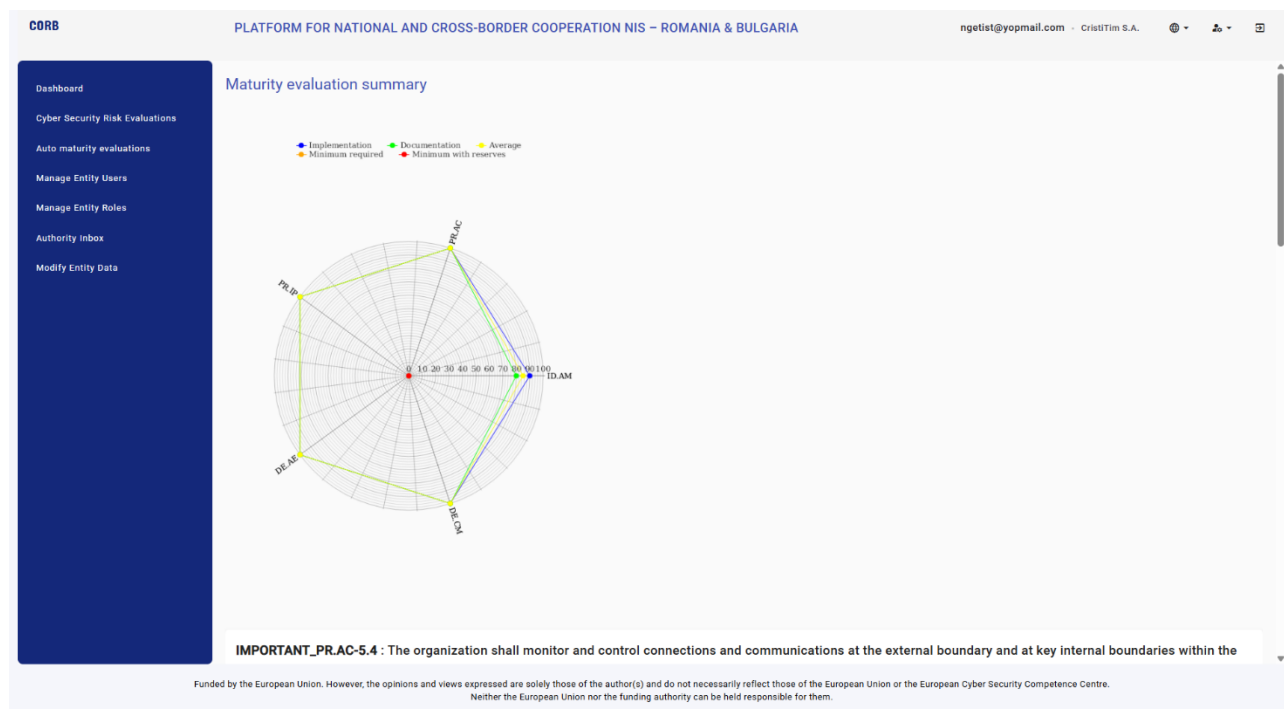


Figure 18. Summary of the maturity assessment

CORB PLATFORM FOR NATIONAL AND CROSS-BORDER COOPERATION NIS – ROMANIA & BULGARIA ngetist@yopmail.com · CristiTim S.A.

Documentation score: 100 of 100
Implementation score: 100 of 100

BASIC_DE.CM-4.1 : Anti-virus, -spyware, and other -malware programs shall be installed and updated.

• Malware includes viruses, spyware, and ransomware and should be countered by installing, using, and regularly updating anti-virus and anti-spyware software on every device used in company's business (including computers, smart phones, tablets, and servers). • Anti-virus and anti-spyware software should automatically check for updates in "real-time" or at least daily followed by system scanning as appropriate. • It should be considered to provide the same malicious code protection mechanisms for home computers (e.g. teleworking) or personal devices that are used for professional work (BYOD).

Documentation score: 100 of 100
Implementation score: 100 of 100

BASIC_PR.AC-4.1 : Access permissions for users to the organization's systems shall be defined and managed.

The following should be considered: • Draw up and review regularly access lists per system (files, servers, software, databases, etc.), possibly through analysis of the Active Directory in Windows-based systems, with the objective of determining who needs what kind of access (privileged or not), to what, to perform their duties in the organization. • Set up a separate account for each user (including any contractors needing access) and require that strong, unique passwords be used for each account. • Ensure that all employees use computer accounts without administrative privileges to perform typical work functions. This includes separation of personal and admin accounts. • For guest accounts, consider using the minimal privileges (e.g. Internet access only) as required for your business needs. • Permission management should be documented in a procedure and updated when appropriate. • Use 'Single Sign On' (SSO) when appropriate.

Documentation score: 100 of 100
Implementation score: 100 of 100

BASIC_PR.AC-1.1 : Identities and credentials for authorized devices and users shall be managed.

Identities and credentials for authorized devices and users could be managed through a password policy. A password policy is a set of rules designed to enhance ICT/OT security by encouraging organization's to: (Not limitative list and measures to be considered as appropriate) • Change all default passwords. • Ensure that no one works with administrator privileges for daily tasks. • Keep a limited and updated list of system administrator accounts. • Enforce password rules, e.g. passwords must be longer than a state-of-the-art number of characters with a combination of character types and changed periodically or when there is any suspicion of compromise. • Use only individual accounts and never share passwords. • Immediately disable unused accounts • Rights and privileges are managed by user groups.

Documentation score: 100 of 100
Implementation score: 100 of 100

IMPORTANT_PR.AC-5.3 : Where appropriate, network integrity of the organization's critical systems shall be protected by (1) Identifying, documenting, and controlling connections between system components. (2) Limiting external connections to the organization's critical systems.

Boundary protection mechanisms include, for example, routers, gateways, unidirectional gateways, data diodes, and firewalls separating system components into logically separate networks or subnetworks.

Documentation score: 100 of 100
Implementation score: 100 of 100

[Download report](#)

Funded by the European Union. However, the opinions and views expressed are solely those of the author(s) and do not necessarily reflect those of the European Union or the European Cyber Security Competence Centre.
Neither the European Union nor the funding authority can be held responsible for them.

Figure 19. Final self-assessment report

➡ Download, re-upload, and submit it for administrator approval.

CORB PLATFORM FOR NATIONAL AND CROSS-BORDER COOPERATION NIS – ROMANIA & BULGARIA ngetist@yopmail.com · CristiTim S.A.

Maturity evaluation [+ Add](#)

Field [Apply Filter](#)

Initiator	Created date	Completion date	Evaluation result Documentation / Implementation	Status	Version	Actions
Ilie Ion	2025-07-31	2025-07-31	98.00% / 99.00%	IN REVIEW	v2025-06-26.2	Edit

Items per page: 5 Page 1 of 1

Funded by the European Union. However, the opinions and views expressed are solely those of the author(s) and do not necessarily reflect those of the European Union or the European Cyber Security Competence Centre.
Neither the European Union nor the funding authority can be held responsible for them.

Figure 20. Final self-assessment / In Review

7.12 Entity dashboard

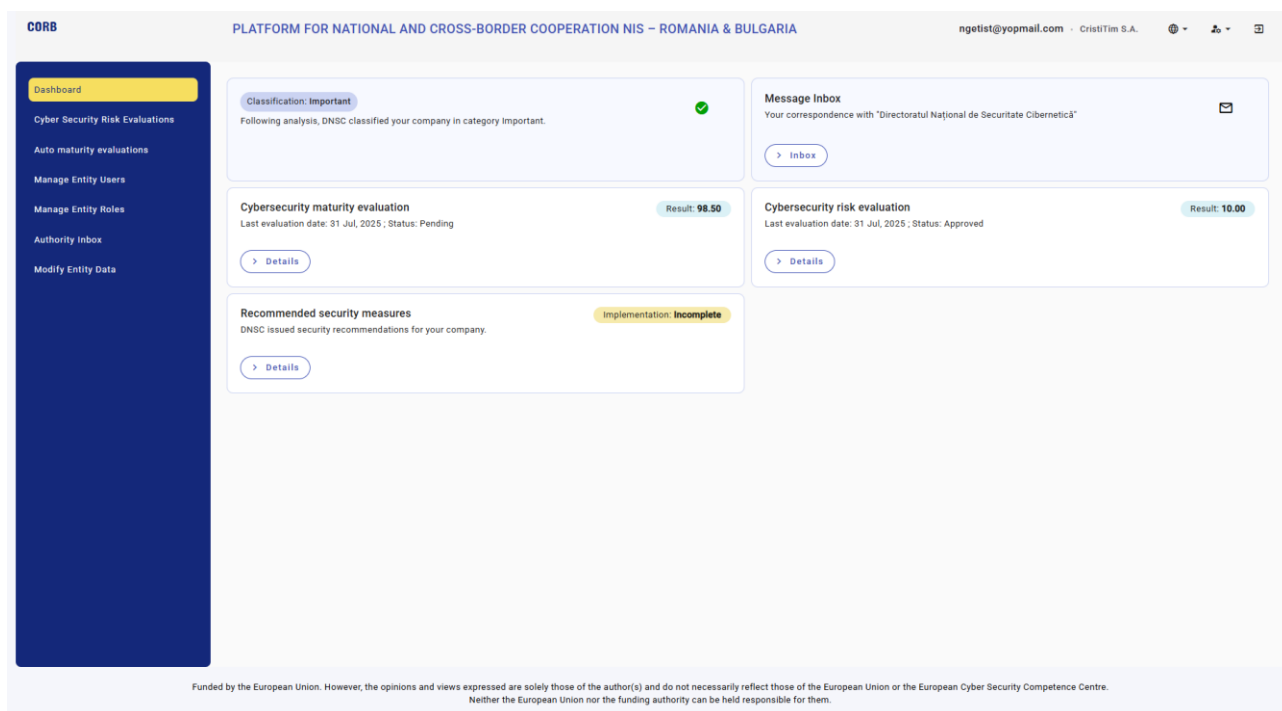


Figure 21. Entity Dashboard

The Dashboard is read-only: it aggregates status information from other modules so you can spot outstanding tasks at a glance.

Coloured badges give instant feedback—green for approved/complete, yellow for items that still need your attention.

Every card provides a **Details** (or **Inbox**) button that takes you directly to the full workflow for that item.

➡ Use the left navigation bar to move between modules without returning to the Dashboard.

7.13 Authority messaging

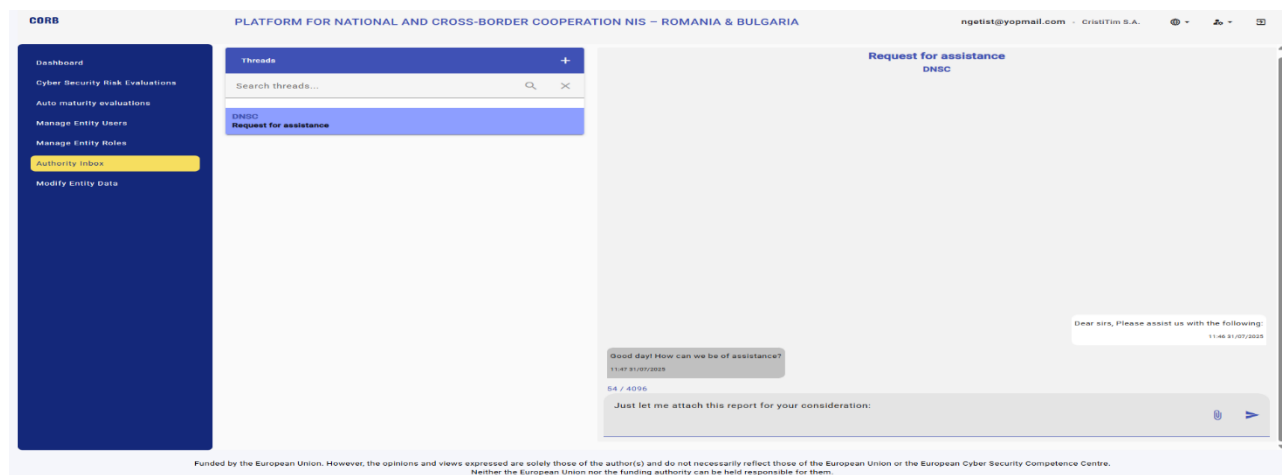
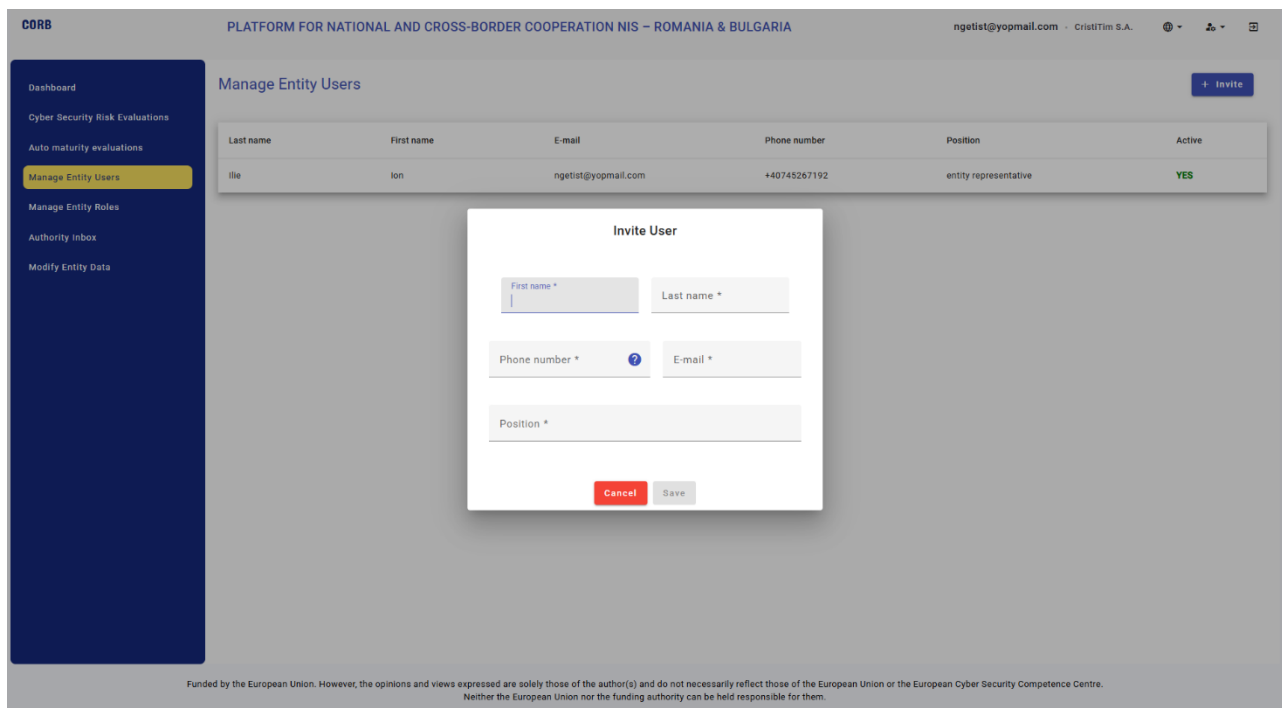


Figure 22. Authority - Entity Messaging Channel

- ➡ To send a new message to the authority press the PLUS sign and enter your message to the Authority.
- ➡ You will be notified when a reply arrives.

7.14 Adding a new user to an existing entity



The screenshot shows the 'CORB' platform interface for 'PLATFORM FOR NATIONAL AND CROSS-BORDER COOPERATION NIS - ROMANIA & BULGARIA'. The user is logged in as 'ngetist@yopmail.com'. The 'Manage Entity Users' section is active, displaying a table with one user: 'Ilie Ion' with email 'ngetist@yopmail.com' and phone number '+40745267192'. An 'Invite User' modal is open, requiring input for 'First name', 'Last name', 'Phone number', 'E-mail', and 'Position'. The 'Save' button is visible at the bottom of the modal.

Figure 23. Adding new users to an existing Entity

- ➡ To add a new user input their contact data and press Save.

Additional Notes

- ❖ All test data is cleared before the platform is launched into production.
- ❖ This process ensures thorough validation of onboarding, risk evaluation, and self-assessment workflows in accordance with NIS2 compliance.

SECTION 8. SECURITY AND CONFIDENTIALITY

Security and data confidentiality are foundational principles in the design and operation of the CORB Platform. Given the sensitive nature of cybersecurity risk data and compliance information, the platform incorporates multi-layered security measures to ensure integrity, confidentiality, availability, and accountability for all data and processes.

8.1. Identity and access management

8.1.1. Authentication

- **Centralized authentication via PAUT:** All users log in through a secure identity provider managed by certSIGN, supporting OAuth2 and OpenID Connect protocols.
- **Multi-factor authentication (MFA):** Mandatory for all users, using SMS tokens or authenticator apps.
- **Password policy enforcement:** Password minimum 12-character length, complexity (uppercase, lowercase, numeric, special character), maximum validity period (90 days), and non-reuse of previous 5 passwords, as aligned with ENISA and NIST SP 800-63B guidelines.

8.1.2. Authorization

- **Role-based access control (RBAC):** Users have access only to features and data necessary for their role (e.g., entity user, authority reviewer).
- **Organization-specific scoping:** Users can only view or manage records related to their organization.

8.2. Data confidentiality and isolation

- **Instance-level isolation:** Romania and Bulgaria each operate separate infrastructure and databases. No data is shared unless explicitly sent via cross-border messaging modules.
- **Encrypted data storage:** Sensitive data is encrypted at rest using AES-256 encryption with key management handled via Hardware Security Modules (HSM) or equivalent certified solutions, ensuring compliance with eIDAS and GDPR requirements.
- **Secure data in transit:** All communication uses HTTPS with TLS 1.3 to protect against eavesdropping and man-in-the-middle attacks.
- **Field-level access control:** Certain high-sensitivity fields (e.g., specific vulnerabilities, assessments) can be hidden from unauthorized roles.

8.3. Secure communication channels

- **End-to-end encrypted messaging:** All cross-border messages between DNSC and MEGBG are transmitted using encrypted peer-to-peer protocols.
- **Session management:** Automatic session timeout and reauthentication required after periods of inactivity.
- **Email and notification security:** Notification services are rate-limited, use SPF/DKIM validation, and include digital signatures where applicable.

8.4. Application security controls

- **Input validation and sanitization:** Prevents XSS, SQL injection, and other common attack vectors.
- **Security headers and CSP:** Enforced HTTP headers (e.g., Content-Security-Policy, X-Frame-Options) mitigate browser-based attacks.
- **Audit logging:** All user actions (login, edits, data views) are timestamped and linked to user identity.

8.5. Infrastructure and hosting security

- **Container isolation:** The application is deployed in Docker containers with strict resource controls and namespace isolation.
- **Host hardening:** Underlying Debian servers are hardened according to CIS Benchmarks, with disabled unused services and firewall rules.
- **Patch management:** Regular updates applied to both host OS and application stack to minimize exposure to known vulnerabilities.
- **Intrusion detection integration:** Optional connection to external SIEM or monitoring systems via API for continuous threat detection. DNSC is implementing this, MEG BG has also this option.

8.6. Data integrity and auditability

- **Usage audit logs:** All user actions within the platform are stored in dedicated logs and can be reviewed by the application administrators and designated users with the necessary RBAC access level.
- **Version control of assessments and risk models:** Each version is stored with timestamp, change history, and user attribution.
- **Backup and recovery:** Regular backups of databases and files with retention policies and tested disaster recovery procedures.

Conclusion

Section 8 demonstrated how a defense-in-depth strategy protected the CORB Platform throughout its lifecycle. Centralized PAUT authentication, mandatory MFA, and strict RBAC confined every user to the minimum privileges required, while instance-level isolation and AES-256 encryption at rest preserved national data sovereignty and GDPR compliance. All traffic travelled over TLS 1.3, and field-level masking further restricted the exposure of sensitive information.

Hardened, containerized hosting, proactive patch management, and optional SIEM hooks reduced infrastructure-level risk, and secure coding safeguards—input validation, CSP headers, and audit logging—shielded the application layer from common exploits. Continuous logging, version control, and tested backup procedures provided full traceability and rapid recovery options.

Collectively, these measures ensured that integrity, confidentiality, availability, and accountability targets were met, giving both Romanian and Bulgarian authorities confidence that the platform remained resilient against evolving cyber-threats while upholding the highest standards of regulatory compliance.

SECTION 9. MAINTENANCE STRATEGY

9.1. Operational maintenance

- **Scheduled updates:** Core platform components, including the frontend, backend, and database layers, are updated regularly with tested patches and feature enhancements.
- **Security maintenance:** Regular vulnerability scans, dependency checks, and penetration tests are conducted. Security patches are applied in accordance with severity classification (critical = immediate, medium/low = scheduled).
- **Monitoring and uptime:** System availability and performance are monitored using container-level and host-level tools. Alerts are generated for downtime, failed services, or unexpected behaviours.
- **Backup & disaster recovery:** Regular automated backups (incremental and full) are configured per instance. Disaster recovery plans are tested biannually.

9.2. Support and helpdesk

- **Tiered support model:**
 - Tier 1: Functional support for platform navigation and user issues
 - Tier 2: Technical debugging and recovery (e.g., form errors, document upload issues)
 - Tier 3: Development support for configuration or code-level defects
- **Issue tracking:** A ticketing system is used to log bugs, feature requests, and enhancement proposals. Each ticket includes severity classification.

SECTION 10. CONCLUSIONS AND WAY FORWARD

The development and deployment of the CORB Platform marks a critical milestone in strengthening cybersecurity collaboration between Romania and Bulgaria in alignment with the NIS2 Directive. By building a secure, modular, and scalable system that supports both national and cross-border coordination, the platform provides a solid foundation for continuous risk management, maturity assessment, and compliance monitoring for food sector entities.

10.1. Conclusions

- The platform successfully supports **secure onboarding, risk classification, self-assessment, and peer coordination** between national authorities.
- **Data segregation, role-based access, and cross-border encrypted messaging** ensure compliance with both NIS2 and GDPR.
- The use of modern architecture (Docker, .NET, Angular, MSSQL) and integration with national infrastructure (e.g., PAUT, RSS) proved robust and maintainable.

10.2. Lessons learned

- **Need for flexibility:** Legislation evolution requires highly configurable templates, workflows, and scoring models that can be adapted without code-level changes.
- **Cross-border challenges:** Legal, linguistic, and procedural differences between countries require careful coordination and dedicated effort.

10.3. Strategic plan for expansion

To align with the full scope of NIS2 and the evolving threat landscape, the Platform will be expanded and continuously improved:

- Sectoral expansion
 - **Short term plan is to onboard** all NIS2-identified operators from all sectors: energy, transport, finance, healthcare, digital infrastructure, public administration, etc.
 - Each new sector will receive customized classification and identification rules as well as risk models tailored to its regulatory context.
- Functional enhancements
 - **Automated threat intelligence feeds** integrated directly into dashboards
 - **Pre-filled assessments and AI-based recommendations** for evidence gathering and control selection
 - **Workflow engines** to automate authority approvals workflow
 - **Keeping up with evolving legislation requirements**
- Commitment to continuous development

The CORB Platform is not a one-time deliverable, but a **living system** that will evolve alongside the cybersecurity ecosystem it supports. The development team and governance structure are committed to:

- Maintaining **technical excellence and security posture of the platform.**
- Supporting **users through training and documentation.**
- Developing the platform with new features and extended capabilities.
- Ensuring that the platform remains **usable, adaptable, and future proof.**

* * *

The official version of the Document is in English, while at the national level, in Romania and Bulgaria, it will be published in the official languages of these countries, namely Romanian and Bulgarian.