INFORB

Implementation of the NIS Directive in the sector production, processing and distribution of food in Romania and Bulgaria.

Project: 101128047 – INFORB – DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE
Participants: DNSC (RO); MEG-BG (BG); CERTSIGN (RO); EXPERTWARE (BE)
Duration: September 2023 – August 2025

Deliverable D5.3. Dissemination and Exploitation Report

DISSEMINATION AND EXPLOITATION REPORT

Document control information

Settings	Value
Document title:	Dissemination and Exploitation Report
Project number:	101128047
Project name:	Implementation of the NIS Directive in the sector production, processing and distribution of food in Romania and Bulgaria.
Acronym project:	INFORB
Author(s) document:	Constantin Călin; Bogdan Radu
Deliverable identifier:	D5.3
Due date of delivery:	29.02.2024
Delivery date:	29.02.2024
Project Manager (MP):	Constantin Călin
Document version:	V1.0
Sensitivity:	PU-Public
Date:	26.02.2024

Document evaluators and evaluators

Name	Role	Action	Date
Constantin Călin	Project Manager	Draft document created	15.02.2024
Bogdan Radu	WP5 Leader	Original version (DNSC)	26.02.2024
Bogdan Radu	WP5 Leader	Open version throughout the implementation of the project.	28.02.2024
Mihai Guranda	Project Assistant Manager	Quality assurance version	28.02.2024
Constantin Călin	Project Manager	Final document assumed and delivered	29.02.2024

Document history

Revision	Date	Created by	Brief description of changes
V0	15.02.2024	Project Manager	Document created
V0.1	26.02.2024	WP5 Leader	Corrigenda updated document with information
V1.0	28.02.2024	WP5 Leader	Update document

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.

Abbreviations

Abbreviation	Name
DER	Dissemination and Exploitation Report
DG CONNECT	Directorate-General for Communications Networks, Content and Technology
ECCC	European Cybersecurity Competence Centre
ECSO	European Cyber Security Organisation
ENISA	European Union Agency for Cybersecurity
EU	European Union
GA	Grant Agreement
INFORB	Implementation of the NIS Directive in the sector production, processing and distribution of food in Romania and Bulgaria
NIS	Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
NIS 2	Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

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.

Summary

The Dissemination and Exploitation Report (DER) is an essential document for this project. Its role is to present clearly and concisely how the project results will be communicated to the target audience and how they will be harnessed to generate the expected impact.

The DER deliverable is mandatory for the INFORB project, developed by the project beneficiaries and uploaded on the SyGMa tool, by the 6th month of this project.

The DER consists of:

(1) The section on communication and dissemination plan.

(2) The section on exploitation.

The first section of the DER presents: objectives, key messages, target audiences, communication channels, planned budget, as well as relevant KPIs. Also, to ensure the communication and dissemination of the results, a social media plan was developed and presented in this deliverable.

The presentation of the results and their exploitation in the next section (section on exploitation) of the deliverable provides the benefits and the possible usefulness also for other sectors/subsectors and other EU member states.

With this DER, it is intended to establish a significant success in disseminating information about the INFORB project and the way of implementing the NIS Directive in the food sector, as well as stimulating the involvement of the target audience. The results of the project will be leveraged by a wide range of stakeholders, contributing to the improvement of the cybersecurity incident management capacity in Romania and Bulgaria, in the food sector.

The project has the purpose to demonstrate the positive impact and to generate valuable recommendations for future cybersecurity initiatives, taking into considerations the impact of the NIS2 Directive on the Digital Market of EU.

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.

Contents

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Section 1. Communication and dissemination plan

Objectives

The main objective of the project *„Implementation of the NIS Directive in the food production, processing and distribution sector – INFORB”* is to strengthen the function of national competent authority for the security of network and information systems of the Romanian National Cyber Security Directorate (DNSC) and the Ministry of Electronic Governance of Bulgaria (MEG-BG), authorities responsible for the implementation of Directive (EU) 2016/1148 and Directive (EU) 2022/2555.

In this respect, the INFORB project aims to support economic entities in identifying them and classifying them as essential and important entities, in a critical sector, to assess and ensure cybersecurity, including the supply chain, namely for the food production, processing and distribution sector (‘food sector’), a new sector established by Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union. The food production, processing and distribution sector is one of the seven economic sectors considered “critical sectors” under the NIS2 Directive.

Both food sector entities and the supply chain need guidance on the implementation of cybersecurity awareness-raising and training programs. In particular, there is a need to clearly define training/education courses in the field of cybersecurity in relation to the different roles and responsibilities in the food sector, as well as cross-border cooperation between the Romanian and Bulgarian national authorities with specific cybersecurity functions and tasks.

The project will develop the “National and Cross-Border Cooperation Platform NIS – Romania and Bulgaria” [CORB], a platform that will ensure:

(1) Supporting the identification and classification of food business entities.

(2) Real-time exchange of information between essential and important entities and the national competent authorities from Romania and Bulgaria on the implementation of the NIS2 Directive.

(3) Cross-border exchange of information in real time between the competent national authorities of Romania and Bulgaria.

In terms of objectives related to the dissemination and exploitation plan, the main objective is *to inform but also to reach out to the society and to show the results of the activities*.

It informs about the usefulness and the benefits of the project for citizens, in particular related to the cyber security of the food sector and supply chain.

At the same time, management awareness and training of staff responsible for cybersecurity in the food sector is one of the specific objectives of the INFORB dissemination and exploitation plan.

Key messaging

According to the guidelines to ensure the publicity and transparency for the European funding, Romanian National Cyber Security Directorate (DNSC) and Bulgarian Ministry of e-governance (MEG-BG) will include publications and dissemination materials on their websites and social media accounts, any brochures or leaflets, reports or internal publications, PowerPoints or graphical presentation, or video and animation.

Regarding DNSC, the information on the INFORB project will be posted on the institution's website (www.dnsc.ro) in the Projects section.

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.

The DNSC, as coordinator, will liaise with DG CONNECT, ECCC, ENISA, ECSO and other relevant parties.

Key messages are essential elements of the Dissemination and Exploitation Plan. They consist of concise, clear and memorable wording that conveys to the target audience the essence of the project, its benefits and the expected impact.

The target messages of the awareness campaign will be centered around the following points:

- Cyber threats and vulnerabilities in the food sector.
- Human factors and institutional organisational strategies for enhancing cyber security.
- Tools, cyber security awareness and training schemes for employees in food sector.
- Engaging with stakeholders of the food sector from Romania to support cyber security challenges and data sharing with the purpose to improve the cyber security in this sector.

The importance of key messages. Key messages – they play a crucial role in the successful dissemination of the project results, with the following benefits:

- **Attraction the attention of the target audience.** Concise and attractive words arise the interest and curiosity of the potential project beneficiaries.
- **Clearly communication of the essence of the project.** The synthesisation of the complex information with the aim of facilitating quick understanding of the project objectives, results and impact.
- **Differentiates the project from other initiatives.** The communication regarding the specificity of the project and the added value that the project brings makes it to stand out in cybersecurity landscape.
- **Stimulates involvement of the target audience.** A well formulated message can encourage the target audience to become actively involved in the project, either by disseminating information or by exploiting the results obtained.

In this sense, the Dissemination and Exploitation Plan of the INFORB proposes the following key messages:

(1) **For the management of food business entities.** *„Investing in cybersecurity education and awareness is critical taking into consideration the protection of the assets, reputation and business continuity. INFORB will introduce the audience into the challenging world of cyber security.”*

(2) For cyber security officers in the food sector. *„Ongoing training and education is the key to stay ahead of the increasing of cyber threats. INFORB will show you what, how and why is necessary to protect the networks and computer systems.”*

(3) **For economic entities in the food sector.** *„Identification and classification as a critical/important entity, determination of cybersecurity maturity level and implementation of cybersecurity requirements are major desiderata set by the NIS 2 Directive. The CORB platform, deliverable of INFORB, is what you need.”*

(4) **For the public.** *„Protect yourself online: be aware of cyber threats and take steps to keep your data and devices safe. INFORB can help you too”.*

At the same time, final key-target messages may result from the deliverables (guidelines, methodologies, checklists, studies and manuals) defined in this project.

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

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.

Target audiences

As far as the audiences (target stakeholder groups) are concerned, they are identified in two groups respectively:

- **Group 1.** Political and governmental institutions (including National Governments, the European Commission and its Agencies).
- **Group 2.** Food professional organizations; Food entities; Research Organizations; Food Academia; General public.

The target audience was grouped in the 2 categories, respectively European/national institutions and entities/persons connected the food sector.

Dissemination activities will be oriented according to these 2 categories.

Informing the entities that carry out activities in the food sector has a particular importance in the process of dissemination and exploitation, regardless of their categorization as essential, important or non-essential entities.

If in the case of group 1 the information and reporting process is important, then in the case of group 2 it is important the process of identifying, preparing, implementing of the cyber security requirements and the level of cyber security maturity.

The level of education of target group 2 must be high and implies at least basic information about cyber security. The dissemination inside the target group 2 gives the necessary support of the implementation of the NIS 2 Directive in the food sector, as well as the rise of the management awareness and the training of the cyber security officers.

Communication channels

Communication channels used for disseminating of the information related to the project include online and offline channels, as well as traditional and other innovative communication methods.

The activities proposed under the Dissemination and Exploitation Plan cover four channels, respectively:

1) Website.
2) Social media.
3) Email.
4) Meeting - physical or online.

Website. The DNSC website [www.dnsc.ro] has a section dedicated to the INFORB project (articles, news, press releases, guides, infographics, etc.).

In the "Projects" section was created the page specific to the "INFORB" project. Information and data about the project are posted here. Also, the main section of DNSC website serves as a central resource for information about the project and its results such as information and press releases.

Email. Special email addresses were created for the project, namely inforb@dnsc.ro and inforb-4all@dnsc.ro used for communications between the consortium members and for communications and disseminations about the project.

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.

Social media. Was created the profile of LinkedIn specifically for the INFORB project: www.linkedin.com/company/inforb-project. Further project-specific profiles and channels will be created on the other social media channels.

Physical or online meeting. Physical (on-site) and online meetings will be held for the dissemination of cyber security information, in order to train cyber security personnel (management and cyber security officers) in food sector entities.

Social media plan

Project: INFORB. Implementation of the NIS Directive in the sector production, processing and distribution of food in Romania and Bulgaria.

Objectives:

- Increasing the visibility of the project and its results at the national (Romania and Bulgaria) and international level.
- Inform about the usefulness and benefits of the project for citizens, especially in terms of cyber security of the food sector and supply chain.
- Inform food entities about the benefits of cyber security and the implementation of minimum-security requirements.
- Ensure compliance with the dissemination requirements imposed by the funding program.

Social Media Channels:

- Facebook
- Twitter
- LinkedIn
- YouTube

Content Types:

Facebook:

- Informative posts about the project, its objectives, implementation stages, and results.
- Blog articles detailing the benefits of using cybersecurity and the protection of networks and information systems to deliver essential/important services.
- Infographics that summarize complex information about the project.
- Interviews with experts involved in the project and with beneficiaries of the implementation of the NIS Directive in the food sector.
- Live Q&A sessions with experts in the field of cyber security, particularly the implementation of the NIS Directive.

Twitter:

- Short and concise posts about project news.
- Messages with relevant hashtags to increase project visibility.
- Retweets of posts from partners and collaborators.

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.

LinkedIn:

- Professional posts dedicated to cybersecurity specialists, especially those in the food sector.
- Opinion pieces on the importance of cyber security, implementation of the NIS Directive and minimum-security requirements.
- Promoting the profiles of experts involved in the project.

YouTube:

- Videos presenting the project and the innovative solution „Platform for national and cross-border cooperation NIS - Romania & Bulgaria [CORB]”.
- Tutorials on the implementation of the NIS Directive, in particular NIS 2, in the food sector.
- Interviews with experts and project beneficiaries.
- Animations and explanatory infographics.

Editorial Calendar:

- Publish a minimum of 1 post per month on each social media platform.
- Adapt the editorial calendar based on the relevant project events, such as start of project, fulfill the tasks from the relevant/specific milestones, achievement of significant results, etc.

Performance Measurement and Evaluation:

- Monitoring KPIs from the GA as well as others such as reach, engagement, click-through rate, etc.
- Use the analysis tools provided by social media platforms to evaluate the effectiveness of campaigns.
- Adapt the social media strategy based on the results obtained.

Additional Considerations:

- Compliance with the branding rules imposed by the funding program.
- Use of a professional and audience-appropriate language.
- Ensuring transparent and open communication.
- Promoting dialogue and interaction with the target audience.

The social media plan is adaptable and flexible being essential to maintain effective online communication throughout the INFORB project.

Adapting the plan to the evolution of the project, audience feedback and the changing context will help to achieve the objectives of dissemination, information and engagement with the target audience.

Social Media Plan Responsible:

- Communication and Public Relations Expert
- WP5 Leader
- Experts/specialists appointed by the consortium partners (MEG-BG, CERTSIGN and Expertware Be).

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Planned budget

Budget Work Package 5
- Cyber awareness programmes and training schemes, as well as an information campaign to introduce the new platform and encourage its use among the stakeholders.

Participants	Costs											
	A. Personnel		B. Subcontracting	C.1 Travel and subsistence	C.2 Equipment	C.3 Other goods, works and services	D.1 Financial support to third parties		D.2 Internally invoiced goods and services	D.3 PAC procurement costs	E. Indirect costs	Total costs
DNSC	10	80.000	-	5.000	-	6.000	-	-	-	-	6.370	**97.370**
MEG-BG	7	45.500	-	5.970	-	30.000	-	-	-	-	5.703	**87.173**
CERTSIGN	4	26.000	-		-		-	-	-	-	1.820	**27.820**
Expertware Be	4	26.000	-		-		-	-	-	-	1.820	**27.820**
Total	**25**	**177.500**	**-**	**10.970**	**-**	**36.000**	**-**	**-**	**-**	**-**	**15.713**	**240.183**

Costs are expressed in EUR.

The budget established for the WP5 action includes both awareness and dissemination actions, as well as training of managers and cyber security professionals from the food sector entities.

Relevant indicators for monitoring and evaluation

In order to establish key performance indicators (KPI's) for communication and dissemination, the following performance indicators were identified to measure the results of communication and dissemination tools:

Communication Activity	Group 1	Group 2	Communication KPI	KPI [target]
Study on cyber security in the sector food (D4.1)	X	X	KPI COMM1: number of downloads	150
			KPI COMM2: number of correspondents	50
Supply Chain Cybersecurity Risk Management Handbook (D4.2)	X	X	KPI COMM3: number of downloads	200
Workshop (T5.2; T5.3)		X	KPI COMM4: number of participants	200
Presentation to relevant events conferences (T5.1)		X	KPI COMM5: total number of events	4
Publications to conferences and journals (T5.1)		X	KPI COMM6: total number of publications	2
Social network dissemination of results (T5.1)		X	KPI COMM7: total number of social network campaigns per year	6

Section 2. Exploitation

The exploitation section describes how the beneficiaries intend to use the results of the INFORB project. (i.e. the deliverables developed which can be used in the food sector and as starting points for all other sectors/sub-sectors of the NIS2 Directive).

A particular importance of the exploration of the INFORB results is the CORB platform (per se), which will be used by the economic entities in the food sector and by the competent authority at national level, but also for cross-border cooperation regarding cyber security in the food sector and the supply chain.

Also, the deliverables could be a part of future secondary legislation of the sectors/subsectors established by the NIS2 Directive based on the transposition laws from Romania and Bulgaria.

Plan for using the results (deliverables)

Methodology regarding the identification and classification of entities in the food sector into essential and important

The identification of economic entities in the food sector and their classification as essential or important is based on NIS2 Directive.

Methodology regarding the identification and classification of entities in the food sector into essential and important (Deliverable D2.1) will resolve the tasks of economic entities in the food sector with regard to the above objectives and will also represent a starting point of the future secondary legislation of the sectors/subsectors established by the NIS2 Directive based on the transposition laws from Romania and Bulgaria.

The methodology will represent a written version for a basic classification of economic entities in essential or important entity based on Annex II from NIS2 Directive "Other critical sectors".

The *Methodology (D2.1)* can be a starting point for the other sectors/subsectors, as well as a guide for the other EU member states.

Good practice guide regarding the implementation of the NIS 2 Directive at the level of the food sector

The need to support entities in the food sector to ensure cyber security, including supply chains, represents the purpose of this deliverable, *Good practice guide regarding the implementation of the NIS 2 Directive at the level of the food sector (Deliverable D2.2)*, which will constitute the basis line for the development/writing of guidelines and good practices for increasing cyber security in the food sector.

The analysis of security risks, the identification of threats and vulnerabilities specific to the food sector, combined with the level of cyber maturity of entities in the food sector (taking into account the operational models for this sector) are lines that will form the basis of the development of the best solutions to ensure sectorial cyber security.

The *Good practice guide (D2.1)* can be a starting point for the other sectors/subsectors, as well as a guide for the other EU member states.

Practical guide to increasing cyber security in organizations and entities in the food sector

Ensuring cyber security at the level of the food sector, including the supply chain, requires support from the competent authority at national level, respectively guidelines and best practices for economic entities in the food sector.

Practical guide to increasing cyber security in organizations and entities in the food sector (Deliverable D2.3) is a guide for entities in the food sector, and not only, in order to increase cyber security.

The *Practical guide (D2.3)* can be a starting point for the other sectors/subsectors, as well as a guide for the other EU member states.

Platform for national and cross-border cooperation NIS – Romania & Bulgaria [CORB]

In order to ensure the identification and record of essential/important entities in the food sector, to ensure the relationship between them and the competent national authorities (Romania and Bulgaria), as well as cross-border cooperation between the two competent national authorities, will be developed the *Platform for national and cross-border cooperation NIS – Romania & Bulgaria [CORB]. (Deliverable D3.1)*.

The *Platform (D3.1)* is an IT application built on 3 sections (modules), respectively (1) identification of food sector entities to which the NIS2 Directive applies; (2) the relationship of the entities with the competent national authority and (3) the RO-BG cross-border cooperation.

The *Platform (D3.1)* presents a core that can be developed to cover, as well all the sectors/subsectors established by the NIS2 Directive and for the transposition of the Directive in the national legislations from Romania and Bulgaria. At the same time, the platform can be integrated into a wider cyber security ecosystem that can include cyber security incident management and cyber crisis situations management.

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.

The *Platform (D3.1)* can be a starting point for the other sectors/subsectors, as well as a guide for the other EU member states.

Study and Handbook regarding cyber security and supply chain for the food sector

Investigating and analyzing the cybersecurity maturity of the ICT infrastructure in the food sector, identifying cybersecurity vulnerabilities in the food-specific supply chain is the key to increase cybersecurity. In this respect, the uniqueness of this project is also *Study and Handbook regarding cyber security and supply chain for the food sector (Deliverable D4.1)* that covers the level of maturity of cyber security and the cyber security risks of the supply chain.

The *Study and Handbook (D4.1)* can be a solution to help all the people responsible for cyber security in the food sector and in the other sectors/sub-sectors established by the NIS 2 Directive and its transposition into national law.

Study and Handbook (D4.1) can be a starting point for the other sectors/subsectors, as well as a guide for the other EU member states.

Training schemes for the management of entities and cyber security professionals in the food sector

The training of the management of the entity and the training of the cyber security professionals in the food sector, are important activities in increasing cyber security in the food sector. *Training schemes for the management of entities and cyber security officers in the food sector (Deliverable D5.2)* are essential in achieving these objectives.

The training sessions will be conducted online/on-site (on the targeted zone of the country) and will be assured by the members of the implementation team or other co-opted experts.

Training schemes (D5.2) can also be used to train staff in other sectors/sub-sectors, as well as being useful for other EU Member States.

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.