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 D1.1. Project Development Plan

PROJECT DEVELOPMENT PLAN

Co-funded by the European Union

Document control information

Settings	Value
Document title:	Project Development Plan
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; Gabriel HÎMPĂ; Gheorghita COMĂNECI
Deliverable identifier:	D1.1
Due date of delivery:	30.09.2023
Delivery date:	20.11.2023
Project Manager (MP):	Constantin CĂLIN
Document version:	V1
Sensitivity:	PU-Public
Date:	17.11.2023

Document evaluators and evaluators

Name	Role	Action	Date
Constantin CĂLIN	MP	Draft document created	03.10.2023
Constantin CĂLIN	MP	Review and Acceptance of Documents	17.11.2023

Document history

Revision	Date	Created by	Brief description of changes
V0	03.10.2023	MP	Document created
V1	17.11.2023	MP	Updated partner information document

Co-funded by the European Union

Abbreviations

Abbreviation	Representing
MP	Project Manager
AMP	Project Manager Assistant
PPE	Project implementation team
EMP	Project Management Team
PC	Consortium partners (DNSC; MEG-BG; CERTSIGN; EXPERTWARE)
PL	Work package
CPL	Coordinator (leader) work package
PDP	Project Development Plan
PLP	Project Plan/Project Work Plan
MMP	Project Management Manual
RRPMR	Risk register and risk minimisation plan

SUMMARY

The Project Development Plan (PDP) is an essential tool for project management and success. It provides a clear map of how the project will evolve and helps maintain a clear direction throughout its implementation.

The document presents the strategic direction and future plans for the implementation of the INFORB project. It aims to provide a vision of how the project will evolve and continue to meet its objectives as it develops.

The first section presents the "Project Plan", i.e. taking into account the scope and tasks of the project, will document the activities needed to achieve the objectives. The document will also serve as a reference for the team and establish ownership of the tasks will divide the project into smaller and more manageable tasks.

The second section presents the "Project Management Manual", respectively will provide an insight into the objectives and structure of the project, as well as the tasks, responsibilities and procedures of the project.

The last section presents the 'Risk register and risk minimisation plan', which provides a specific risk management framework, i.e. risk identification and to ensure a minimisation of risks for each phase of the project.

PDP is an essential management document used to achieve the objectives of the INFORB project and can be updated throughout the project lifecycle by PM, with the contribution of the project team.

Co-funded by the European Union

"Co-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. Neither the European Union nor the granting authority can be held responsible for them."

Contents

PROJECT WORK PLAN

Co-funded by the European Union

1. Introduction

The **Project Work Plan (PLP)** is a detailed document that specifically describes how the different stages and activities of a project will be carried out in order to achieve the objectives set. This is an essential management tool to ensure that the project is delivered in time, budget and with the desired quality.

In these circumstances, the PLP is a crucial tool for the efficient management of the INFORB project, a complex project with cross-border impact, in order to achieve the objectives set.

The scope and tasks of the project were taken into account in the development of the PLP and also the documentation of the activities necessary to achieve the objectives. The document will also serve as a reference for the team and establish ownership of tasks.

The PLP is a document developed to detail the activities and tasks of the project, documenting each action to achieve the objectives set out in the INFORB project.

As necessary, the PLP can be updated throughout the project lifecycle by PM, with the contribution of the project management team.

2. Detailed structuring of activities

WP/T		Activities	Steps (sub-activities)	Responsible	Participants
WP1.		**Project management and coordination.**		**C. Calin**	
1	**1.1**	Project management and monitoring.	Bi-weekly meetings, and whenever needed, with the project consortium	C. Calin	MG. Guranda
			Weekly meetings with the project management team	C. Calin	MG. Guranda G. Himpa G. Comăneci BA. Radu FJ. Kalleder
			Organising and conducting opening, finalising and/or intermediate meetings with the entire consortium.	C. Calin	MG. Guranda
			Establish the operational working of the PPE and mobilise team members to achieve the assigned tasks.	C. Calin	MG. Guranda
			Elaboration of deliverables established for WP1, i.e. Project Development Plan (PDP), Progress Report and Final Report.	C. Calin	MG. Guranda G. Himpa G. Comaneci
			Planning and monitoring the implementation of actions	C. Calin	MG. Guranda G. Himpa G. Comaneci BA. Radu FJ. Kalleder
			Prepare monthly documents related to the implementation and payment process.	C. Calin	N. Roman
			Reporting and relations with the EC on the state of implementation of the project.	C. Calin	AC. Vasilescu MG. Guranda
	1.2	Risk management and quality assurance.	Monitoring risks with a view to minimising them.	C. Calin	MG. Guranda
			Verification and quality assurance of documents/working steps.	C. Calin	MG. Guranda N. Roman

WP/T		Activities	Steps (sub-activities)	Responsible	Participants
WP2.		**Food business entities and relationship with the national competent authority.**		**G. Himpa**	
2	**2.1**	Establishing criteria for identifying essential and important entities.	Analysis of the requirements set out in the NIS2 Directive with a view to classifying economic operators as essential or important entities for the food business.	G. Himpa	BA. Radu SN. Dorobanțu
			Develop and validate the list of criteria and specifications for the identification of essential and important entities.	G. Himpa	SN. Dorobanțu MG. Guranda
			Classification of food business entities. Classification criteria and categories.	G. Himpa	SN. Dorobanțu C. Calin
			Development, validation and teaching of 'Methodology on the identification and classification of food business entities in essential and important'.	G. Himpa	SN. Dorobanțu C. Calin MG. Guranda
			Identification and establishment of channels for dissemination and access to methodology by food business operators.	G. Himpa	SN Dorobanțu
	2.2	Develop guidelines on the implementation of the NIS 2 Directive in the food sector.	Establish the structure of the guide and the responsibilities of the experts involved in the elaboration of the guide.	G. Himpa	C. Calin MG. Guranda
			Collection and analysis of relevant documents from project partners, including published studies and post-publication conclusions.	G. Himpa	SN Dorobanțu
			Development and validation 'Guide to Good Practice on the implementation of the NIS 2 Directive at the level of the food sector'.	G. Himpa	SN. Dorobanțu C. Calin MG. Guranda
			Finalising, teaching and disseminating the 'Guide to Good Practice on the implementation of the NIS 2 Directive at the level of the food sector'.	G. Himpa	SN Dorobanțu
	2.3.	Developing best practices for increasing cybersecurity in the food sector.	Establish the structure of the guide and the responsibilities of the experts involved in the elaboration of the guide.	G. Himpa	C. Calin MG. Guranda
			Networking with food business entities and consortium partners, identifying and collecting information necessary to develop the guide.	G. Himpa	SN Dorobanțu MG. Guranda
			Development and validation of the "Practical Guide to Increasing Cybersecurity in Food Business Organisations and Entities".	G. Himpa	SN. Dorobanțu C. Calin MG. Guranda

WP/T		Activities	Steps (sub-activities)	Responsible	Participants
			Finalising, teaching and disseminating the 'Practical Guide to Increasing Cybersecurity in Food Business Organisations and Entities'.	G. Himpa	SN Dorobanțu
	2.4.	Evaluation of documents on the implementation of the NIS Directive in the food sector.	Assessment and identification of the needs of food business entities for the implementation of the NIS2 Directive. Updating the documents.	G. Himpa	SN Dorobanțu
			Develop and provide food entities with compliance checklists useful for the implementation of the NIS2 Directive in the food sector.	G. Himpa	SN Dorobanțu
WP3.		**Development of an information and cooperation platform.**		FJ. Kalleder	
3	**3.1**	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.	FJ. Kalleder	C. Calin MG. Guranda
			Development of diagrams, sketches and interfaces necessary for the operation of the platform.	FJ. Kalleder	SN Dorobanțu
			Establish security requirements and technologies used to develop the CORB platform.	FJ. Kalleder	SN. Dorobanțu C. Calin MG. Guranda
			Define and establish the cooperation between the developer and the beneficiary's representative.	FJ. Kalleder	C. Calin SN Dorobanțu
			Establish the testing and validation requirements of the platform, as well as those for revision, approval, update and change management.	FJ. Kalleder	C. Calin SN Dorobanțu
	3.2	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.	FJ. Kalleder	SN Dorobanțu
			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.	FJ. Kalleder	SN Dorobanțu
			Regular meetings between the beneficiary's representative and the CORB platform development team.	FJ. Kalleder	SN Dorobanțu
			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.	FJ. Kalleder	SN Dorobanțu

WP/T		Activities	Steps (sub-activities)	Responsible	Participants
	3.3.	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.	FJ. Kalleder	SN. Dorobanțu G. Himpa G. Comaneci
			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).	FJ. Kalleder	SN. Dorobanțu
			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.	FJ. Kalleder	SN. Dorobanțu G. Himpa G. Comaneci BA Radu
			Validation of platform functionality and performance. Security assessment. Testing the capacity and ease of operation of the platform.	FJ. Kalleder	SN. Dorobanțu G. Himpa G. Comaneci
WP4.		**Cybersecurity at the level of economic entities, including supply chain**		**G. Comaneci**	
4	**4.1**	Survey of food business entities on the security of network and information systems used for the provision of essential/important services.	Identification of the target group for conducting the survey (name, category, field of activity/CAEN, contact). Establishing the modalities of sending/receiving questionnaire replies (e-mail, web forms, letrics, telephone, online platform managed by partners if they have). Establishing the format, modalities for recording, storing, processing the content of questionnaires.	G. Comaneci	N. Roman SN. Dorobanțu BA Radu FJ. Kalleder
			Preparation, review and validation of the content of the questionnaire within the PPE. (EUSurvey platform)	G. Comaneci	C. Calin MG. Guranda N. Roman
			Application of questionnaires and collection of relevant information. Augmenting the database and saving the data collected for processing.	G. Comaneci	N. Roman FJ. Kalleder
	4.2	Develop the analysis on cybersecurity in the food sector.	Analysis of the information collected and the documents related to the questionnaires. Proposals to improve/review the questionnaire.	G. Comaneci	C. Calin MG. Guranda

WP/T		Activities	Steps (sub-activities)	Responsible	Participants
			Assessment of the situation in Romania regarding cybersecurity in the food sector.	G. Comaneci	G. Himpa BA. Radu SN Dorobanțu
			Elaboration and validation of the study containing conclusions on cybersecurity in the food sector.	G. Comaneci	C. Calin MG. Guranda
			Submit study to project partners and request feedback. Collecting, discussing feedback and developing the final form.	G. Comaneci	N. Roman
			Publication on the INFORB website of the 'Study on Cybersecurity in the Food Sector'. Preparation of feedback questionnaire. Electronically disseminating the study by e-mail at least to the target group and requesting feedback. Collecting and processing feedback.	G. Comaneci	SN Dorobanțu FJ. Kalleder N. Roman
			Completion and handover of the deliverable "Study on Cybersecurity in the Food Sector".	G. Comaneci	
	4.3.	Development of the cybersecurity risk management manual specific to the food supply chain.	Establish the structure of the manual and responsibilities of PPE members.	G. Comaneci	C. Calin MG. Guranda
			Collection and analysis of relevant documents from project partners, including published studies and post-publication conclusions.	G. Comaneci	N. Roman FJ. Kalleder SN. Dorobanțu
			Development and validation of "Cybersecurity Risk Management Manual in the Supply Chain".	G. Comaneci	C. Calin MG. Guranda
			Completion, handover and dissemination of the deliverable "Cybersecurity Risk Management Manual in the Supply Chain".	G. Comaneci	MG. Guranda
	4.4.	Development and validation of cybersecurity compliance lists at production, processing and distribution stages.	Develop compliance lists in the field of cybersecurity at the production, processing and distribution stages.	G. Comaneci	G. Himpa BA Radu
			Finalising, publishing and/or submitting compliance lists to partners and requesting feedback. Analyse feedback and update lists.	G. Comaneci	BA Radu SN Dorobanțu
WP5.		**Awareness and training programmes in the field of cybersecurity. Inform stakeholders about the new platform and encourage its use.**		**BA. Radu**	

WP/T		Activities	Steps (sub-activities)	Responsible	Participants
5	5.1	Awareness of food business entities and the public.	The choice of strategies and means for developing and implementing the awareness plan.	M. Rotariu	C. Calin MG. Guranda BA Radu
			Finalising, handing over and disseminating the deliverable “Awareness Plan”.	M. Rotariu	BA Radu MG. Guranda C. Calin
			Development and development of an INFORB website (component of CORB platform) and dissemination of awareness material.	M. Rotariu	BA Radu G. Comaneci SN Dorobanțu
			Implementation of the Awareness Plan.	M. Rotariu	BA Radu
	5.2	Training of the management of food business entities.	Identification and involvement of key stakeholders. Identifying and determining the beneficiaries of training programs.	BA. Radu	C. Calin MG. Guranda G. Comaneci
			Elaboration of presentation and study materials for management training in the food sector.	BA. Radu	G. Himpa G. Comaneci FJ. Kalleder
			Establishing the locations and how to carry out the training programs.	BA. Radu	G. Comaneci N. Roman
			Provision of training workshops for the management of food business entities.	BA. Radu	G. Himpa G. Comaneci FJ. Kalleder SN. Dorobanţu
			Collect and centralise feedback from workshops. Analysis.	BA. Radu	N. Roman
			Completion, teaching and dissemination of ‘Training programmes for the management of entities and cybersecurity officers in the food sector (entity management component)’.	BA. Radu	G. Himpa G. Comaneci MG. Guranda
	5.3.	Training of cybersecurity staff in the food sector.	Identification and involvement of key stakeholders. Identifying and determining the beneficiaries of training programs.	BA. Radu	C. Calin MG. Guranda G. Comaneci

WP/T		Activities	Steps (sub-activities)	Responsible	Participants
			Development of presentation and study materials for the training of cybersecurity officers in the food sector.	BA. Radu	G. Himpa G. Comaneci FJ. Kalleder
			Establishing the locations and how to carry out the training programs.	BA. Radu	G. Comaneci N. Roman
			Providing training workshops for cybersecurity officers in the food sector.	BA. Radu	G. Himpa G. Comaneci FJ. Kalleder SN. Dorobanțu
			Collect and centralise feedback from workshops. Analysis.	BA. Radu	N. Roman
			Finalising, teaching and disseminating 'Training programmes for the management of entities and cybersecurity officers in the food sector (cybersecurity component)'.	BA. Radu	G. Himpa G. Comaneci MG. Guranda

3. Deliverables

Deliverable No.	Name	Delivery time
D1.1.	Project Development Plan	M1
D1.2.	Interim report	M12
D1.3.	Final report	M24
D2.1.	Methodology for identifying and classifying food establishments into essential and important.	M7
D2.2.	Guide to good practice on the implementation of the NIS 2 Directive at the level of the food sector.	M14
D2.3.	Practical Guide to Increasing Cybersecurity in Food Organisations and Entities.	M20
D3.1.	Platform for national and cross-border cooperation NIS – Romania and Bulgaria [CORB].	M21

Deliverable No.	Name	Delivery time
D4.1.	Study on Cybersecurity in the Food Sector.	M15
D4.2.	Supply chain specific cybersecurity risk management manual.	M20
D5.1.	Awareness plan	M2
D5.2.	Training programmes for the management of entities and cybersecurity officers in the food sector.	M23

4. Budget

PARTICIPANTS	COSTS [EUR]									
	A. Personal		B. Subcontracting	C.1 Transport and daily subsistence allowance	C.2 Equipment	C.3 Other supplies, works and services	D.1 Financial support for third parties	D.2 Goods and services with domestic billing	E. Indirect costs	Total costs
WP1. Cybersecurity at the level of economic entities, including supply chain										
DNSC	10	80.000		2.000		3.000			5.950	**90.950**
MEG-BG	6	39.000		1.800					2.856	**43.656**
CERTSIGN	4	26.000		1.000					1.890	**28.890**
Expertware Be	2	13.000		1.000					980	**14.980**
Total WP1	**22**	**158.000**		**5.800**		**3.000**			**11.676**	**178.476**
WP2. Food businessentities and relationship with the national competent authority.										

PARTICIPANTS	COSTS [EUR]									
	A. Personal		B. Subcontracting	C.1 Transport and daily subsistence allowance	C.2 Equipment	C.3 Other supplies, works and services	D.1 Financial support for third parties	D.2 Goods and services with domestic billing	E. Indirect costs	Total costs
DNSC	8	64.000		2.000		2.000			4.760	**72.760**
MEG-BG	5	32.500							2.275	**34.775**
CERTSIGN										
Expertware Be										
Total WP2	**13**	**96.500**		**2.000**		**2.000**			**7.035**	**107.535**
WP3. Development of an information and cooperation platform.										
DNSC	8	64.000			2.000	1.000			4.690	**71.690**
MEG-BG	5	32.500			2.500				2.450	**37.450**
CERTSIGN	27	175.500		5.000				30.000	14.735	**225.335**
Expertware Be	5	32.500		1.000					2.345	**35.845**
Total WP3	**45**	**190.000**		**6.000**	**4.500**	**1.000**		**30.000**	**24.220**	**370.220**
WP4. Food businessentities and relationship with the national competent authority.										
DNSC	14	112.000		2.000		1.000			8.050	**123.050**
MEG-BG	8	52.000		2.500					3.815	**58.315**
CERTSIGN	4	26.000							1.820	**27.820**
Expertware Be										
Total WP4	**26**	**190.000**		**4.500**		**1.000**			**13.685**	**209.185**

PARTICIPANTS	COSTS [EUR]									
	A. Personal		B. Subcontracting	C.1 Transport and daily subsistence allowance	C.2 Equipment	C.3 Other supplies, works and services	D.1 Financial support for third parties	D.2 Goods and services with domestic billing	E. Indirect costs	Total costs
WP5. Awareness and training programmes in the field of cybersecurity. Inform stakeholders about the new platform and encourage its use.										
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 WP5	**25**	**177.500**		**10.970**		**36.000**				**240.183**
OVERALL TOTAL	**131**	**855.000**		**29.270**	**4.500**	**43.000**		**30.000**	**72.328,90**	**1.105.598,90**

5. Activity Chart

ACTIVITIES	MONDAY																						
	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14	M15	M16	M17	M18	M19	M20	M21	M22	M23	M24
T1.1. Project management and monitoring.																								
T1.2. Risk management and quality assurance.																								
T2.1. Establishing criteria for identifying essential and important entities.																								

ACTIVITIES	MONDAY																						
	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14	M15	M16	M17	M18	M19	M20	M21	M22	M23	M24
T2.2. Develop guidelines on the implementation of the NIS 2 Directive in the food sector.																								
T2.3. Developing best practices for increasing cybersecurity in the food sector.																								
T2.4. Evaluation of documents on the implementation of the NIS Directive in the food sector.																								
T3.1. Development of operational requirements for the development of the CORB cooperation platform.																								
T3.2. Development and operationalisation 'Platform for national and cross-border cooperation NIS – Romania & Bulgaria [CORB]'.																								
T3.3.Testing and validating the CORB cooperation platform.																								
T4.1. Survey of food business entities on the security of network and information systems used for the provision of essential/important services.																								
T4.2. Develop the analysis on cybersecurity in the food sector.																								
T4.3. Development of the cybersecurity risk management																								

Co-funded by the European Union

"Co-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. Neither the European Union nor the granting authority can be held responsible for them."

ACTIVITIES	MONDAY																						
	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14	M15	M16	M17	M18	M19	M20	M21	M22	M23	M24
manual specific to the food supply chain.																								
T4.4. Development and validation of cybersecurity compliance lists at production, processing and distribution stages.																								
T5.1. Awareness of food business entities and the public.																								
T5.2. Training of the management of food business entities.																								
T5.3. Training of cybersecurity staff in the food sector.																								

Co-funded by the European Union

PROJECT MANAGEMENT MANUAL

Co-funded by the European Union

"Co-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. Neither the European Union nor the granting authority can be held responsible for them."

1. Introduction

The Project Management Manual (MMP) is a detailed and structured document that provides a comprehensive description of how the project will be managed, executed and monitored throughout its duration. This document serves as a guide to all aspects of project management and is an essential reference resource for the project implementation team and stakeholders.

The MMP provides a solid framework for efficient project management and ensuring that it is delivered in time, budget and with the desired quality. It is an essential tool for clearly communicating the plan and ensuring that everyone involved in the project has a common understanding of how it will be managed and implemented.

In the development of the MMP it was taken into account that project management must be an essential process that brings clarity, efficiency and coherence in the management of the INFORB project. MMP is also a vital reference resource for the success of the project and for ensuring that all key aspects of the project are properly and professionally managed.

The development of the MMP involved consideration of several key aspects to ensure the success of the project and an efficient management of the project.

The implementation of the NIS 2 Directive in the 'Food Production, Processing and Distribution' sector in Romania and Bulgaria is a complex and important project to ensure cybersecurity in this critical sector in ensuring food resilience.

The project management manual is a dynamic document and will be updated throughout the project lifecycle as needed.

As required, MMP – a dynamic document will be updated throughout the project lifecycle. Whenever the document is updated, stakeholders will be informed of the changes made.

Co-funded by the European Union

2. Overview of the project

2.1. Project Summary

The **project "Implementation of the NIS Directive in the food production, processing and distribution sector - INFORB" aims**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, authorities responsible for the implementation of Directive (EU) 2016/1148 and Directive (EU) 2022/2555.

INFORB 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 in the Union. The food production, processing and distribution sector is one of the seven economic sectors considered "critical sectors" under the NIS2 Directive.

Food sector entities as well as the supply chain need guidance on the implementation of cybersecurity awareness and training programmes. In particular, it is necessary to define the necessary cybersecurity training courses 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 authority in 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 view of the visibility of the project and its good recognition at the level of the food sector, the INFORB project can also be presented through the logo built for this purpose, namely:

The relevant key performance indicators for measuring the results of the INFORB project are related to the following aspects:

- **KEY PERFORMANCE INDICATOR 1: Achievements in the implementation of the objectives and requirements of the NIS Directive and the NIS 2 Directive in relation to the food sector:**
  - ✓ *KPI 1: identification and involvement of 50 food business entities.*

- **KEY PERFORMANCE INDICATOR 2: Achievements in the uptake in food business entities, in particular SMEs, of dedicated (cross-border) cybersecurity tools, methods, organisational and management practices, including peer-to-peer information exchange:**
  - ✓ *KPI 2: carrying out at least 150 downloads of project results from the web portal that will support the uptake of dedicated (cross-border) cybersecurity (cross-border) cybersecurity tools, methods, organisational and management methods, methods, practices, including peer-to-peer information exchange.*

- **KEY PERFORMANCE INDICATOR 3: Achievements in (cross-border) cybersecurity education, awareness raising and skills development in food sector entities:**
  - ✓ *KPI 3: representatives (specialists and/or management) from at least 50 food business entities participating in total in the training workshops. The workshops will take place on both sides of the border, in the cross-border region, with expert exchange and information events presented (when practical and applicable to the subject) by both members of the DNSC and the Bulgarian Ministry of Electronic Governance.*

2.2. Project data

General	Details
Project number	101128047
Project name	Implementation of the NIS Directive in the food production, processing and distribution sector in Romania and Bulgaria
Acronym project	INFORB
Duration	24 months
Estimated costs	EUR 1 105 598,90
Maximum EU grant amount	EUR 572 460,70
Participants	NATIONAL CYBERSECURITY DIRECTORATE MINISTRY OF EGOVERNMENT CERTSIGN'S EXPERTWARE BELGIUM

2.3. Critical Success Factors

We appreciate that the most important factors for the success of the INFORB project are:

1) Involvement of stakeholders and acceptance of project objectives.

The EIP will ensure communication and active involvement in the project.

The critical success factor is the willingness and capacity of consortium partners to help relevant stakeholders increase resilience, in the context of the implementation of the NIS2 Directive.

2) Team involvement and ability to prioritise tasks and meet deadlines.

This critical success factor will be achieved by ensuring close monitoring of tasks and implementation of the work plan by the project management team.

3) Effective communication between PPE members.

Essential to achieving this goal will be to ensure frequent and close communication between the project implementation team members and the management team, especially the project manager.

2.4. Project stakeholders

Stakeholders	Role	Description	Interest	Influence
MP	Key role	It has key tasks in the overall success of the project and the coordination of the project at consortium level. Ensures the monitoring and management of the INFORB project.	High	Raised

Stakeholders	Role	Description	Interest	Influence
AMP	Key role	It has a key role in managing the successful performance of PPE tasks, project quality assurance and communication with European bodies.	High	Raised
EMP	Key role	EMP will be directly involved in the management of objectives throughout the project duration and will be the key driver of the project's success, along with PM and AMP.	High	Raised
PPE	Key role	PPE plays a key role in achieving the objectives (WP) by providing expertise and carrying out tasks, achieving the planned steps (sub-activities).	High	Raised
Consortium partners	Key role	They are key facilitators that provide their own project teams and give added weight to the INFORB project when contacting stakeholders outside the institutions. The partners have a direct interest in the success of the project and in the resilience of the food sector in Romania and Bulgaria.	High	Raised
Food business entities	Lead role	Both private and food sector institutions are the main beneficiaries of the project and will be directly affected by the outcome of INFORB.	High	Average
Specialists in ensuring cybersecurity in the food sector	Lead role	Key to implementing the findings of the INFORB project and best practices and providing information on current trends and vulnerabilities that have an impact on the food sector. The involvement of a key number of specialists will be essential for the achievement of the project objectives and implementation at entity level, as well as for ensuring resilience in the sector.	Environment	Average
Management of food business entities	Secondary role	Involving the management of entities both in their training and in the implementation of the NIS2 Directive at the level of food business entities will ensure the success of this project.	Environment	Low
Independent experts	Optional role	Co-opting independent experts can be one of the main objectives of the project. Experts will provide advice throughout the project lifecycle.	Low	Average
Food trade associations or organisations	Optional role	While not directly affected, their involvement will have an impact on the overall success of the project and provide valuable feedback and information on the state of food cybersecurity.	Low	Low

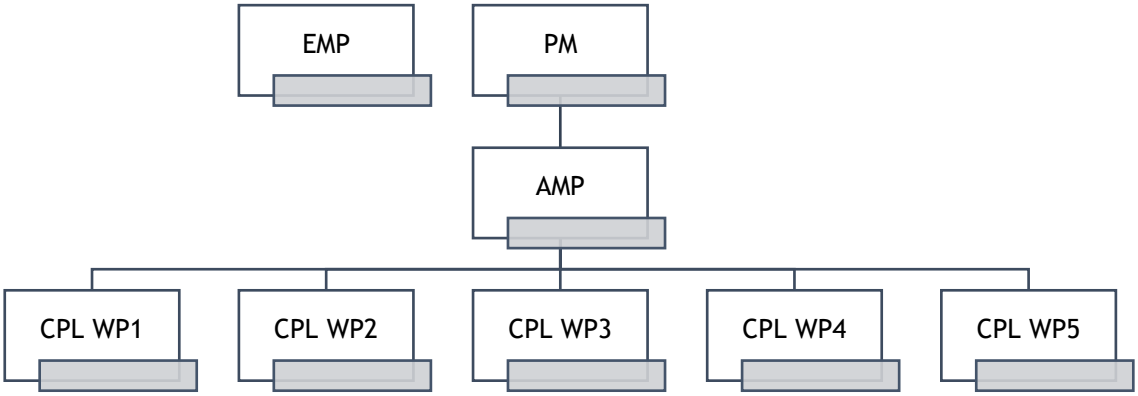
Co-funded by the European Union
"Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them."

3. Roles, responsibilities and management structure

3.1. Management bodies

To increase efficiency and communication between teams, project management will be structured on the following levels: (1) first level – the project will be coordinated by PM and AMP. (2) Second level – work packages (WP) will be coordinated by a CPL. It should be noted that the two levels will constitute EMP.

The project coordination structure is presented in the following diagram:



3.2. Project Manager

The**project manager** will supervise the project on a daily basis, coordinate the project implementation team and ensure the efficient allocation of resources to achieve high quality results. It will also ensure coordination of the project at consortium level.

Specific responsibilities within the INFORB project will be:

(a) Organisation of start-ups, final project review and regular team meetings;
(b) Coordinating the project implementation team and ensuring the efficient allocation of resources;
(c) Coordination of the project at consortium level;
(d) Identifying and agreeing on the main stakeholders and contacts of the INFORB project;
(e) Mobilising the project team;
(f) Communication and liaison with INFORB logistics;
(g) Developing a detailed work plan with the stakeholder matrix, tasks, milestones, results, data and resources;
(h) Establishing workflow communication and risk management plans;
(i) Establishing the operational working of the project team;
(j) Planning and monitoring of project implementation;
(k) Preparation and transmission of status reports, stage checks and reimbursement claims.

The project manager will communicate closely with AMP, CPL and EMP. Also, for the successful implementation of the project, PM will cooperate and work closely with CPL.

3.3. Project Manager Assistant

The Project Manager Assistant will ensure communication with European bodies and external partners in the consortium. It will also provide regulatory and legal expertise.

Specific responsibilities for AMP:

(a) Direct coordination and communication with the European Commission;
(b) Overseeing the overall progress of the project;
(c) Responsible for the quality of the results. Ensuring and monitoring the quality of documents/materials produced during the project;

(d) Making suggestions for possible changes to the work plan;
(e) Monitoring contact with stakeholders;
(f) The INFORB project documents will be submitted to the European Commission by AMP, together with the project implementation expert.

3.4. Coordinators(s) of the work package

The coordinators/leaders of the work packages (for each package) will ensure the timely execution of the tasks included in each work package and monitor the effective implementation of the work plan and objectives of the project.

The CPL will communicate closely the PM and the APM, ensure a constant flow of information on the status of the respective work package, the status of the tasks and the effectiveness of the implementation of the tasks.

3.5. Project Management Team

The project management team will ensure the analysis and verification of the status of the project, by stages of implementation and according to the project implementation deadlines.

The EMP will also analyse the risks identified during the project and set out measures to minimise them.

4. Project procedures

4.1. Project communication

Ensuring effective communication between project team members and external entities will be one of the key factors in the success of the INFORB project implementation.

For optimal communication and permanent access to information and documents needed to implement INFORB, a common work area has been created in SharePoint. A repository of documents for project results, reports and other relevant documents was implemented in MS Teams (INFORB team) and each team member was informed about the mailing lists of other project participants.

4.1.1. Internal communication

The section deals with communication between project team members. It consists of electronic mail, online and in-person meetings.

(a) Repertoire of project documents

- Documents will be stored and shared in collaboration in the repository that has already been created. The exchange of relevant documents will enhance internal communication within the PPE and allow for rapid and efficient exchange of information.
- The documents uploaded to the register will comply with the general rules referred to in section 3.4.2. of the project manual.
- The link to the project repository that has been configured will be made available to all EIP members, i.e.: INFORB.

(b) Emails

- A list of all PPE members has been established and is available to all participants. Any modification of the PPE shall be communicated and appropriate modifications shall be made.
- An email group, INFORB, has been created with related email address: inforb@dnsc.ro.
- The project management team will send priority emails to all team members with responsibilities relevant to the subject. In order to ensure a constant flow of information, support management

and make appropriate changes to project documents, correspondence will be carried by email between team members (PM, AMP and CPL).

- E-mails will be marked as urgent in case of emergency and with the necessary action if the recipient has to take action.
- In order to ensure their visibility and optimal management, all emails related to the project will be prefixed to the subject: "INFORB – 101128047/".

List of DNSC project team members:

Name	Role	Contact
Constantin CALIN	Project Manager (MP)	0740-101.361; 0748-250.710 constantin.calin@dnsc.ro
George-Mihail GURANDA	Project Manager Assistant/ Regulatory and Legal Expert (AMP)	0722-265.853 mihai.guranda@dnsc.ro
Gabriel HIMPA	WP2 Coordinator	0723-681.950 gabriel.himpa@dnsc.ro
Gheorghita COMANECI	WP4 Coordinator	0722-241.547 gheorghita.comaneci@dnsc.ro
Bogdan-Alexandru RADU	WP5 Coordinator	0743-114.417 bogdan.radu@dnsc.ro
Friedrich-Josef KALLEDER	Coordinator WP3/ Cybersecurity expert (app development networking)	0745-267.192 josef.kalleder@dnsc.ro
Silviu-Nicolae DOROBANTU	Cybersecurity expert	0730-131.476 silviu.dorobantu@dnsc.ro
Alina VASILESCU	Expert project implementation (EC networking)	0725-203.387 alina.vasilescu@dnsc.ro
Mihai ROTARIU	Communication expert	0740-066.866 mihai.rotariu@dnsc.ro
Narcissa ROMAN	Financial control and financial reporting on the project	0785-257.444 narcisa.roman@dnsc.ro

(c) Meetings

- Meetings of PPE. They will be organised in advance and the agenda for the meeting will be established and made available to all EIP members involved. The meetings will be followed by minutes of meetings prepared by the host of the meeting, which will be short and concise and include relevant details of the agenda, participants and main conclusions.
- The EMP meetings. Project progress meetings will take place at least every 2 weeks and involve the entire EMP team.
- B2B meetings. It will be organised at the request of the EMP members, with the nominated PPE staff, in order to identify solutions and set deadlines for carrying out the tasks.
- Avoid organising meetings that are not necessary to promote more efficient time management.
- Meetings/meetings will take precedence in the following way:
  - Meetings on the progress of the project, where the progress of the project will be discussed and the applicable achievements and deadlines will be reviewed.
  - Other meetings, on cross-working groups, specific working groups or involving the whole PPE. Meetings will take place if it is considered relevant to organise specific discussions or to plan certain parts of the work.

(d) Online meetings

"Co-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. Neither the European Union nor the granting authority can be held responsible for them."

- Continuous communication between EIP members is one of the critical success factors of the project and a way to ensure that the project objectives are achieved. To ensure fruitful collaboration and constant flow of information, frequent meetings between EIP members and/or EMP INFORB will take place to monitor progress, coordinate work and support project management in general.
- To ensure quick communication, the preferred way will be to organise online meetings. This will facilitate the integration of EIP members working remotely and reduce the impact on project costs. The platform for organising team meetings will be Microsoft Teams.

(e) Personal Meetings (B2B)

- Personal meetings are important to support project management, as they allow EIP members to hold in-person discussions, promoting better cooperation and more committed participation from all involved.
  - In order to reduce the impact of the costs of personal meetings, they will preferably take place at DNSC headquarters in str. Italian, No. 22.
- In addition, at the level of the consortium partners, their own PPE meetings will preferably take place at their premises.
- So far, meetings have taken place with the project team:
  - Launch meeting – September 2023;
  - Meetings between: MP, AMP, CPL on project status and task analysis.

4.1.2. External communication

External communication involves communication with stakeholders outside the project team. Communicating the project with external entities will be essential for the success of the project and for the involvement of stakeholders.

An effective communication and awareness strategy will also be developed and implemented by the communication expert involved in the project as part of task 5.1, in order to develop and maintain an outreach strategy for cybersecurity and food communities, involving them and setting out the reasons for early adoption of the project results.

The Communication Expert will ensure effective information between partners as well as between stakeholders and announce updates on the implementation of the project using established communication channels.

4.2. Preparation and presentation of results

The results will be reviewed after completion by at least one PPE member to ensure early identification of errors and the result to be in line with the standard. The team member who is in charge of completing the activity will upload the deliverable to the common area “INFORB” (MS Teams) for review.

The reviewer will complete the document table at the beginning of the “authorisation and reviewers”, their name, role in the project, actions taken (approved, peer reviewed, etc.) and date of review.

When identifying documents/results, the following scheme will be used: [DX.Y] [name of deliverable] [Version].

The recommended font for documents will be Trebuchet MS.

Prior to validation and submission/submission results, a final review will be carried out to ensure that the results are in line with the objectives and description, that a linguistic check has been carried out, that no significant defects have been identified and that they are ready for delivery.

In case of delays, the MP will be informed to provide an explanation of the delay. After quality verification, AMP and MP will be responsible for the final submission of the result.

4.3. Project monitoring and reporting

Regular reporting of progress will be essential for monitoring the progress of projects, achievements and difficulties in each task.

Each member of the PPE will report on the progress of the tasks to the CPL and the AMP.

In order to ensure the success of the project, the CPL will have meetings with experts at least every 2 weeks to review progress in implementation, roadblocks, risks and risk mitigation and to report on the expected performance of the tasks.

The project manager will prepare and report on progress at mid- and end-of-implementation period (to the EC) and monthly (to the head of the institution – director of DNSC).

MP will be kept informed by the CPL of delays in the overall project as well as of each work package that can be submitted, including progress in tasks.

4.4. Quality assurance and control

The project quality management process comprises activities and procedures designed to meet quality expectations. Responsible for the quality of the results is AMP.

Since most of the results of the INFORB project will be in the form of reports/results, the main objective of quality assurance in the INFORB project is to ensure a high quality of documents, both in terms of relevance and form.

Also, the software development of the CORB Platform, its testing and validation are key objectives of the project, and quality assurance and control are important tasks of AMP and CPL (WP3).

4.4.1. Responsibilities:

Each CPL will be responsible for the quality of the results in the work packages it coordinates. It is the responsibility of the project manager to meet the overall project quality expectations, and AMP is responsible for the quality of the results presented to the European Commission.

4.4.2. Types of documents

The main types of documents that will be produced during the INFORB project will be deliverables, evaluation reports, meeting minutes and presentations.

Also, one of the essential deliverables is the CORB Platform.

In order to allow interoperability and ease of use of documents, all documents must be produced in MS Word. When working in collaboration on the official document, actions such as suggesting changes to documents and peer reviews should be followed in the same document.

In general, the name of the documents should be carried out as follows:

- Mention the type of document: whether the document is part of a work package, deliverable, minutes of the meeting or other.
- The title of the document in a way that provides a basic description of its content.
- Version number. The version will start at 0 (v.0) for anticipated projects and 1, 2, 3 for later versions; it will be incremented by 0.1 for minor changes and 1.0 for major changes by the PPE member making the change.

4.4.3. Quality control of deliveries

The results should be assessed 'inter peer' to ensure that they meet the necessary quality standards. The members of the PPE reviewing the document should follow their actions in the document that has been amended.

4.4.4. Internal quality control

AMP will assess quality control activities and assess compliance with the plans in terms of scope, time, cost, quality, project organisation and risks. Project risks, problems and decision changes will be documented by the project manager.

In order to ensure quality control of specific tasks and results, quality control topics will be discussed at regular meetings to assess the development of the identified risks of the project and the measures to be taken.

The produced documents shall be peer reviewed at least once by a member of the PPE, taking into account the following aspects:

- the document should be easily understandable and legible;
- there should be no spelling or grammatical errors;
- the document must contain all the necessary sections.

4.4.5. Feedback

Internal quality control will consist of quality assurance, by following the development of the project, providing feedback and validating the procedures and conclusions reached.

5. Managing risks and problems

Risk management, identification and mitigation will be ensured throughout the project lifecycle in order to control the risks and problems that may arise and which will have an impact on the actual implementation of the project. The project manager is responsible for ensuring that a risk management process is implemented and followed.

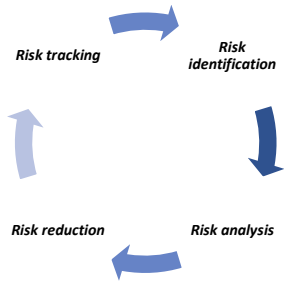
The risk will be continuously monitored to identify new risks and mitigation measures, and the risk register and risk minimisation plan will be continuously updated with the risks and mitigation measures arranged.

5.1. Risk monitoring process

All PPE members shall be responsible for identifying and assessing risks and providing contingency plans to minimise them.

Risks and possible situations that can be identified as risks will be regularly discussed during EMP meetings/meetings. The team will brainstorm on potential risks and minimisation measures.

Whenever a PPE member identifies risks, they shall be reported to the PM and to the coordinator/leader of the work package and shall ensure that they have taken note of this issue.



Risk monitoring will be a continuous process, including risk tracking to monitor how the risk minimisation plan is implemented and to monitor results, risk identification, risk assessment and risk mitigation measures.

5.2. Risk register

The Risk Register and risk minimisation plan for the INFORB project were created.

It is the responsibility of the PM to ensure that measures are taken to monitor, identify, assess and minimise risks, as well as to update the MRR.

The registry and plan will be uploaded to the common INFORB space (from MS Teams) in SharePoint and will be known to the entire PPE.

The RRPMR will facilitate the application of minimisation measures by the whole team in the event of a risk and will ensure that the whole team is aware of the risk minimisation measures.

5.3. Risk minimisation actions

Strategies that will be used to address risks will be risk avoidance and risk minimisation.

Taking action to avoid risks will be the preferred method to be used for the project.

Strategies for each specific risk will be discussed with the members of the PPE concerned and risk mitigation measures will be assigned, implemented and known to the parties involved.

5.4. Problem management

The responsibility of the project manager is to identify and address. If, the problems cannot be solved at the EMP level they will be escalated to a higher level.

The issues will also be discussed and recorded in the minutes of the EMP meeting/meetings. Consideration will be given to identifying solutions to solve them.

Taking into account the number of stakeholders involved and the scale of the project, the problems will be addressed in a timely manner and there is no need for a complex procedure.

In order to prevent problems arising between PPE and EMP members, transparent communication will be the main approach of this project.

Co-funded by the European Union

RISK REGISTER AND RISK MINIMISATION PLAN

Co-funded by the European Union

"Co-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. Neither the European Union nor the granting authority can be held responsible for them."

1. Introduction

The **Risk Register and Risk Mitigation Plan (RRPMR)** is a key document in project management. This document aims to identify, assess and manage potential risks that may affect the INFORB project and develop strategies to minimise their impact. The importance of this document is to:

RRPMR is a key tool in the management of INFORB, as it helps to identify, assess and manage risks effectively to ensure that the project is successfully delivered in time and budget. This document contributes to a more efficient management of uncertainties and to reduce the likelihood of failure of the project.

In conclusion, the RRPMR is an essential tool for the success of the project. This document not only identifies potential risks, but also develops detailed plans to manage them effectively, thereby reducing uncertainties and problems throughout the project. The main aspects taken into account in the development of the MRR were: comprehensive identification of risks, prioritisation of risks, allocation of adequate resources to minimise and continuous monitoring of the situation. Communication and stakeholder involvement are also crucial. Flexibility and lifelong learning are also important for improving the risk management process in INFORB.

The INFORB Project Implementation Team (EIP) will consider that the risks may be uncertain events or conditions that, upon occurrence, may produce a negative impact (threats) or positive (opportunities – innovation potential) on at least one project objective (e.g. costs, graph, scope). The project risk management process aims to minimise the impact of negative risks. Risk management (risk identification, analysis and classification, monitoring, definition of mitigation actions and reporting) was carried out as part of project management (WP1) and will be analysed/addressed during the meetings of the project management team. The identified risks and the minimisation plan will be part of the regular project reports.

Depending on the needs, the RRPMR can be updated throughout the project lifecycle by the PM, with the contribution of the project management team.

2. RISK MANAGEMENT PROCESS

The risk management process within the INFORB project is a systematic and planned approach to identify, assess, manage and monitor risks that may affect the success or objectives of the project. This process aims to minimise negative risks and exploit opportunities to ensure successful completion of the project.

PMR is essential in achieving project objectives (WP) and can have a significant impact on its success.

The aim of the RMP is to minimise or manage risks in an efficient manner so as to reduce the negative impact on the objectives of the INFORB project.

2.1. Risk identification

During the development phase of the project, several risks and minimisation measures were identified and included in the grant agreement, which can be found in the “Critical Risks List” section on page 83.

In the implementation phase of the project, the focus will always be on identifying and minimising risks, which will be discussed during the regular meetings of the EMP.

The main focus will be on:

- status of deliverables;
- the achievement of the objectives;
- regular communication between EMP, CPL and PPE;
- continuous monitoring of the timetables and scope of the work package.

Co-funded by the European Union

“Co-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. Neither the European Union nor the granting authority can be held responsible for them.”

Risk identification and mitigation were discussed at a meeting between the EMP.

2.1.1. Risk assessment

MP will be responsible for identifying and ensuring risk response, while EMP will be responsible and constantly involved in identifying and responding to risks. PPE members will be informed and consulted on risks and mitigation options.

The occurrence of risks will be discussed during the periodic meetings of the PPE and will be estimated using the Low/Environment/High scale.

2.1.2. Risk management

Risk response involves identifying measures to address risks in terms of progress and expected results of the project. Each identified risk will be assigned a risk officer, i.e. a risk response.

The risk officer. It will be responsible for the supervision and reporting of risks, as well as for taking appropriate and timely action.

The Project Manager. It will be responsible for carrying out project risk management and for monitoring and responding to risks in all project activities. Updating the RRPMR is the responsibility of the project manager.

Project management team. It will be responsible for the overall guidance of the team and the fulfilment of the obligations and responsibilities imposed by the European Commission. It will be responsible for monitoring and responding to risks.

Coordinators(s) of work packages. They will be responsible for the implementation of the work within their own work package and are responsible for the specific risks and results expected in their working group. If new risks are identified, they should inform the EMP and MP, which will update the risk management table.

2.1.3. Response strategy

Avoiding. The most desirable action is to avoid possible risks. This will be achieved through constant communication within the project.

Mitigation. If a threat cannot be completely avoided, the risk will be minimised in accordance with the actions listed in the Risk Register.

2.1.4. Monitoring the implementation of control measures

The status and effectiveness of the risk mitigation plan should be communicated to the MP in order to update the risk register and to assess the efficiency of the instruments and measures taken.

The risk officer will confirm the correct implementation of the risk response and verify the effectiveness of the response. It will also monitor the situation and inform the MP. In turn, the MP will inform and discuss with the EMP on risk events, minimisation plans and implementation effectiveness.

The risk exposure will be constantly reassessed and monitored. The new risks will be analysed and added to the Risk Register.

The risk register will be discussed at the EMP project meetings and will be constantly updated. The updates will also contain relevant issues that occurred during the project implementation phase and possible risk avoidance or mitigation measures.

Co-funded by the European Union

"Co-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. Neither the European Union nor the granting authority can be held responsible for them."

3. RISK REGISTER

Risk No.	Description	Probability level	WP	Risk minimisation measures (proposed)
1	Limited access to organisational maturity and operational models of food business entities	Low	WP2 WP3 WP4	There are different organisational maturities and operating models that can be adapted to food business entities. DNSC is the national competent cybersecurity authority in accordance with the NIS Directive 2 and Government Emergency Ordinance 104/2021 for the food production, processing and distribution sector – as such, it has direct access to food business entities in relation to cyber aspects. DNSC also has its own approach that supports the development of strategies in the national civilian cyberspace, including in the food sector. DNSC has successfully applied this approach to public and private sector actors to gain insight into organisational and operational maturity, organisational and operational models. The Ministry of Electronic Governance is the counterpart of the DNSC in Bulgaria, with the necessary regularity powers and authority to collect and process information related to cyber security and resilience. A coherent and all-encompassing approach to reaching stakeholders will be applied for maximum coverage of the initiative in the food sector.
2	Limited access to information about cybersecurity awareness and training.	Low	WP5	DNSC has extensive experience in providing cybersecurity training for professional networks. This allows them to have access to available materials on training programmes. The Bulgarian partner has extensive experience in capacity building initiatives and a wide network of experts at its disposal to guarantee the implementation of the training programme.
3	Limited access to information about cyber threats, vulnerabilities and related incidents in the food sector entities.	Low	WP3 WP5	DNSC has expertise in cybersecurity. They are aware of the main sources of cybersecurity information. The Bulgarian partner will hire a number of experts to carry out in-person surveys and face-to-face meetings with SMEs, to better understand the situation in terms of cybersecurity preparedness and to get a personal impression on the steps needed to achieve the level of resilience objectives. Project partners will constantly monitor professional communication channels, including reports and news published by national cybersecurity authorities in the European Member States, the CSIRTs network, sectoral CSIRTs.
4	Risk that work packages and project tasks will not be completed on time – failure to meet deadlines.	Low	WP1 WP2 WP3 WP4 WP5	We have adopted a project management methodology based on PM²/PRINCE2® and we will apply it strictly to ensure that project tasks and deliverables are carried out in the manner required and at the expected quality level. Proper and strict time management will apply – we will plan all project activities in advance and set up a reserve for delays, unforeseen events, diseases and so on.

Risk No.	Description	Probability level	WP	Risk minimisation measures (proposed)
5	The risk that deliverables are not met, expectations, quality and acceptance criteria.	Moderately	WP1 WP2 WP3 WP4 WP5	This risk will be avoided by a clear, mutually agreed definition of objectives, scope of each work package and tasks. If, however, a difference in expectations occurs during a mission, the escalation process will allow early warning of problems. We will then try to adjust the project to address the difference. If necessary, we can change the composition of the working group of the project team in order to strengthen a field perceived as weak, or invest more time in a particular field of work. We will appoint a project manager and a quality assurance agent with great experience.
6	Risk of unexpected unavailability of staff.	High	WP1 WP2 WP3 WP4 WP5	Every effort will be made to ensure a minimum interruption in the event of unforeseen events, unforeseen unavailability (e.g. illness, etc.). In the unlikely event of unavailability, substitutes will be found - we will ensure that the necessary skills and expertise are covered. DNSC will ensure the redundancy of resources and the necessary level of expertise in case of unexpected occurrence of an unexpected unavailability of any expert in the core team. The Bulgarian Ministry envisaged a subcontracting of the most time-consuming tasks (investigations and meetings with SMEs) of external experts. The unavailability of an expert will not be a problem due to their interchangeability. The basic expertise required for data analysis will be provided by the staff of the Ministry's team, made up of long-term experts with proven experience in the partner's team.

4. RISK MINIMISATION PLAN

Risk No.	Materialisation of risk	Risk minimisation measures (taken)
1	NO	There is no need for action.
2	NO	There is no need for action.
3	NO	There is no need for action.
4	NO	There is no need for action.
5	NO	There is no need for action.
6	NO	There is no need for action.

"Co-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. Neither the European Union nor the granting authority can be held responsible for them."
Co-funded by the European Union