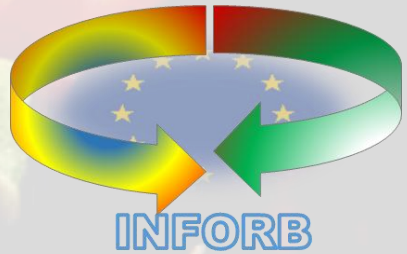
DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

REPUBLIC OF BULGARIA
MINISTRY OF ELECTRONIC GOVERNANCE

certSIGN epertware

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



PROJECT:
101128047 – INFORB – DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE

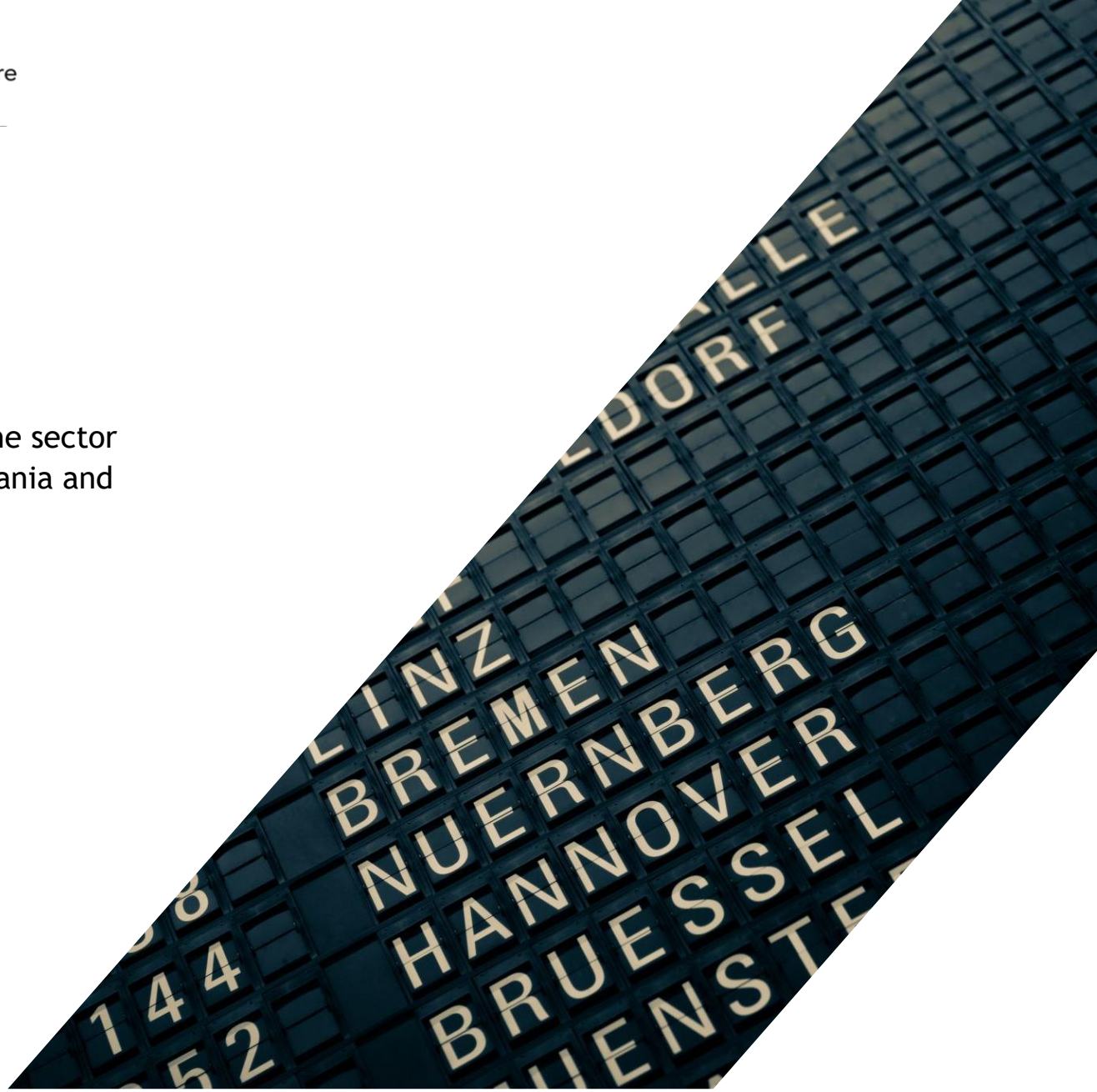
Co-funded by the European Union

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.

Project Details

- Project Name: Implementation of the NIS Directive in the sector production, processing, and distribution of Food in Romania and Bulgaria
- Project Acronym: INFORB
- Call: DIGITAL-ECCC-2022-CYBER-03
- Topic: DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE
- Type of Action: DIGITAL-JU-SME
- Service: CNECT/H/01
- Project Starting Date: September 1, 2023
- Project Duration: 24 Months



Introduction

- Welcome to our project presentation, "Implementation of the NIS Directive in the sector production, processing, and distribution of Food in Romania and Bulgaria"
- Our project aligns with the NIS 2 Directive and takes on critical cybersecurity challenges in the food sector
- Now, let us tackle the serious business of cybersecurity, and remember, no fishing allowed!

PROJECT:
101128047 – INFORB – DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE
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.

Introduction

- **Definition:** As per Regulation (EC) No 178/2002 of the European Parliament and of the Council, 'food business' is defined as any undertaking, whether for profit or not and whether public or private, engaged in activities related to any stage of production, processing, and distribution of food.
- **Scope:** This definition includes a wide range of entities involved in the food sector, including:
  - Wholesale Distribution: Entities engaged in the distribution of food products on a large scale.
  - Industrial Production: Businesses involved in large-scale food production and processing.

PROJECT:
101128047 – INFORB – DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE
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.

Project Objectives

- Enhance cybersecurity within the food sector to safeguard vital infrastructure, including networks and IT systems
- Identify, assess, and manage vulnerabilities specific to the food supply chain, minimizing cybersecurity risks
- Develop comprehensive cybersecurity compliance lists for various stages of food production, processing, and distribution

PROJECT:
101128047 – INFORB – DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE
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.

Consortium Partners

DNSC - **DIRECTORATUL NATIONAL DE SECURITATE CIBERNETICA**

BGMEG - **MINISTRY OF ELECTRONIC GOVERNANCE**

CSGN - **CERTSIGN SA**

EXPTBE - **EXPERTWARE BELGIUM**

PROJECT:
101128047 – INFORB – DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE
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.

Work Package Structure

- WP1: Project Management
- WP2: Economic Entities and Classification
- WP3: Cooperation Platform Development
- WP4: Cybersecurity Assessment
- WP5: Awareness and Training

INFORB
PROJECT:
101128047 – INFORB – DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE
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.

Work Package 1 - Project Management

Tasks in WP

- Project coordination, planning, and monitoring
- Timely reporting to stakeholders and financiers
- Risk assessment and management

Key Outcomes

- Ensured project stays on track and within budget
- Transparent communication among consortium members
- Prompt issue resolution and adaptive project management

INFORB
PROJECT:
101128047 – INFORB – DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE
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.

Work Package 2 - Economic Entities and Classification

Tasks in WP

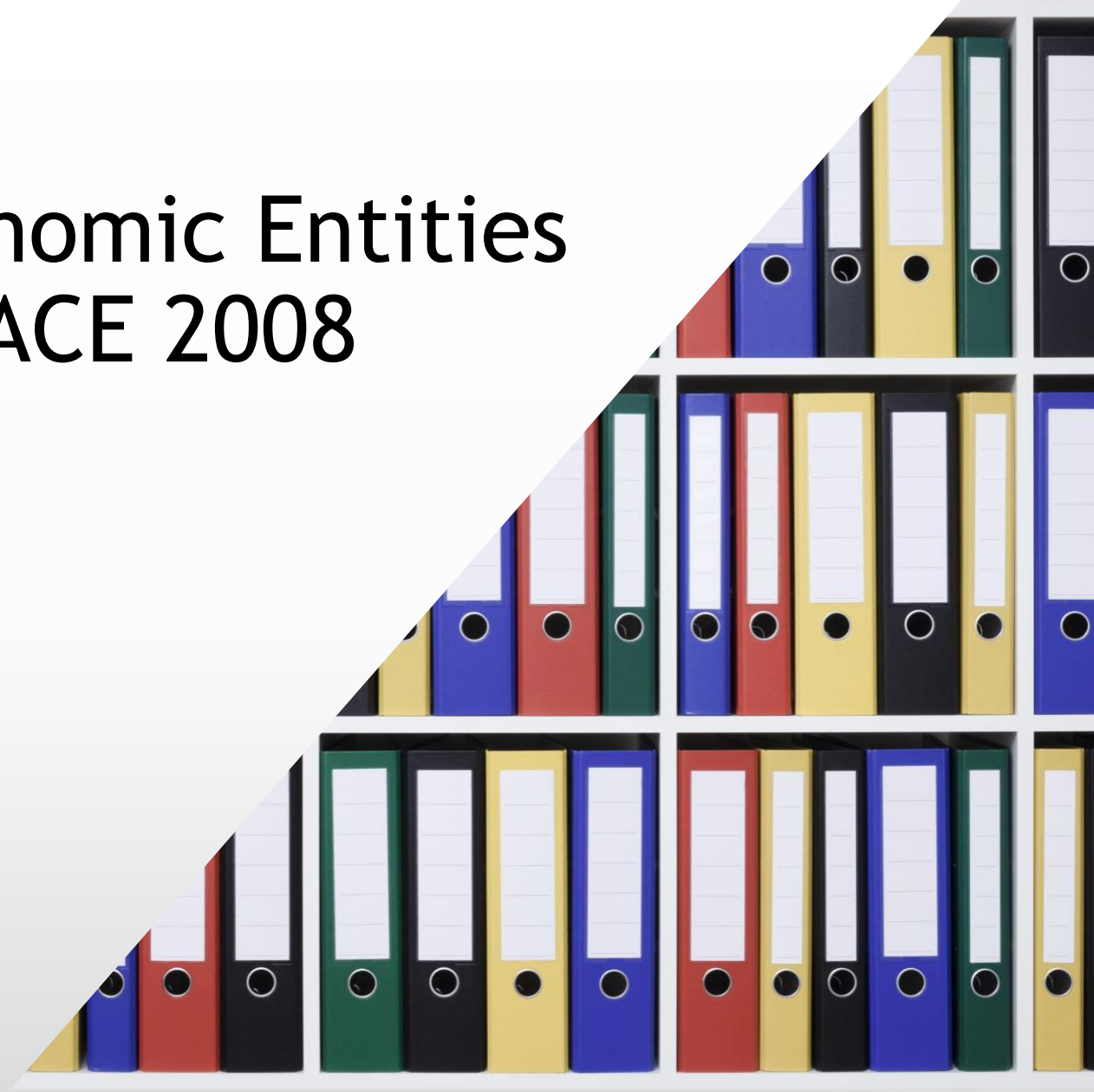
- Identifying and classifying food sector entities
- Developing criteria for entity classification
- Creating methodology for sector-specific entity identification

Key Outcomes

- Methodology for consistent identification and classification of essential and important entities in the food sector. For Bulgaria is published here: https://egov.government.bg/wps/portal/ministry-meu/home/programs.projects/projects-progress/digitaleurope

INFORB
PROJECT:
101128047 – INFORB – DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE
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.

Work Package 2 - Economic Entities and Classification – NACE 2008



- Section C - Manufacturing
  - Division 10 – Groups 10,1; 10,2; 10,3; 10,4; 10,5; 10,6; 10,7; 10,8
  - Division 11 – Group 11
- Section G – WHOLESALE AND RETAIL TRADE
  - Division 46 – Groups 46,1; 46,3
  - Division 47 – Groups 47,1; 47,2; 47,8 и 47,9
- Section H – TRANSPORT AND STORAGE
  - Class 52,10 - Storage
- Section I – HOTELS AND RESTAURANTS
  - Division 55 – Group 55,1
  - Division 56 – Groups 56,1; 56,2; 56,3 и 56,4

PROJECT:
101128047 – INFORB – DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE
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.

Work Package 3 - Cooperation Platform Development

Tasks in WP

- Defining operational requirements for the CORB cooperation platform
- Developing and operationalizing the cross-border cooperation platform
- Testing and validation of the CORB cooperation platform

Key Outcomes

- Enhanced cross-border collaboration
- Efficient information exchange among stakeholders
- A secure and operational cooperation platform

INFORB
PROJECT:
101128047 – INFORB – DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE
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.

Work Package 4 - Cybersecurity Assessment

Tasks in WP

- Conducting surveys on food sector entities' network security with link: https://ec.europa.eu/eusurvey/runner/7c850660-723e-fa51-245b-7669caabe0a3
- Analyzing cybersecurity status and vulnerabilities
- Developing a cybersecurity risk management manual for the supply chain

Key Outcomes

- Cybersecurity risk management manual for the supply chain for:
  - Minimizing risks in the food supply chain
  - Comprehensive risk management procedures

PROJECT:
101128047 – INFORB – DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE
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.

Work Package 5 - Awareness and Training

Tasks in WP

Conducting awareness workshops for food sector entities

Developing training schemes for entity management

Providing training for personnel responsible for cybersecurity

Key Outcomes

Improved cybersecurity awareness among food establishments

Enhanced cybersecurity skills for entity management and staff

A more resilient and prepared food sector

PROJECT:
101128047 – INFORB – DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE
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.

Project Milestones

Project Kick-off and Planning	Project plans and baselines
Reporting to the European Commission	The coordinator has reported on the project to the European Commission
Guidelines for NIS Directive	Documents on the implementation of the NIS Directive in the food sector
Platform Ready for Use	Operationalization of the platform
Enhancing Cybersecurity	Evaluation of cybersecurity and supply chain for the food sector
Awareness Initiatives	Planning awareness activities
Cybersecurity Training	Training of personnel with attributions in cybersecurity management for the implementation of the NIS2 Directive

PROJECT:
101128047 – INFORB – DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE
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.

Deliverables

- D2.1: Methodology for Entity Classification (WP2) - Publicated
- D2.2: Good Practice Guide for NIS 2 Directive Implementation (WP2) - Developed
- D2.3: Practical Guide for Cybersecurity in the Food Sector (WP2) - Developed
- D3.1: CORB Cooperation Platform (WP3) – under implementation
- D4.1: Cybersecurity Study and Handbook (WP4) – to be elaborated
- D5.1: Awareness Plan (WP5) - under implementation
- D5.2: Training Schemes for Food Sector Cybersecurity (WP5) - under implementation

PROJECT:
101128047 – INFORB – DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE
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.

Cybersecurity in the Food Sector

- Consumer Safety: Cyberattacks can lead to tampering with food products, potentially endangering consumer health

PROJECT:
101128047 – INFORB – DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE
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.

Project Impact

- Enhanced Food Safety: By strengthening cybersecurity measures, we reduce the risk of tampering and contamination of food products, ensuring consumer safety
- Increased Trust: Improved cybersecurity builds trust among consumers, stakeholders, and partners in the food sector, enhancing the sector's reputation
- Business Resilience: Food establishments with robust cybersecurity practices are more resilient to cyber threats, safeguarding their operations and profitability
- **Regulatory Compliance: Our project assists food entities in complying with cybersecurity regulations, mitigating legal risks**

PROJECT:
101128047 – INFORB – DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE
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.

Project Impact

- Cross-Border Collaboration: The development of the CORB cooperation platform promotes cross-border collaboration, sharing best practices, and bolstering collective security

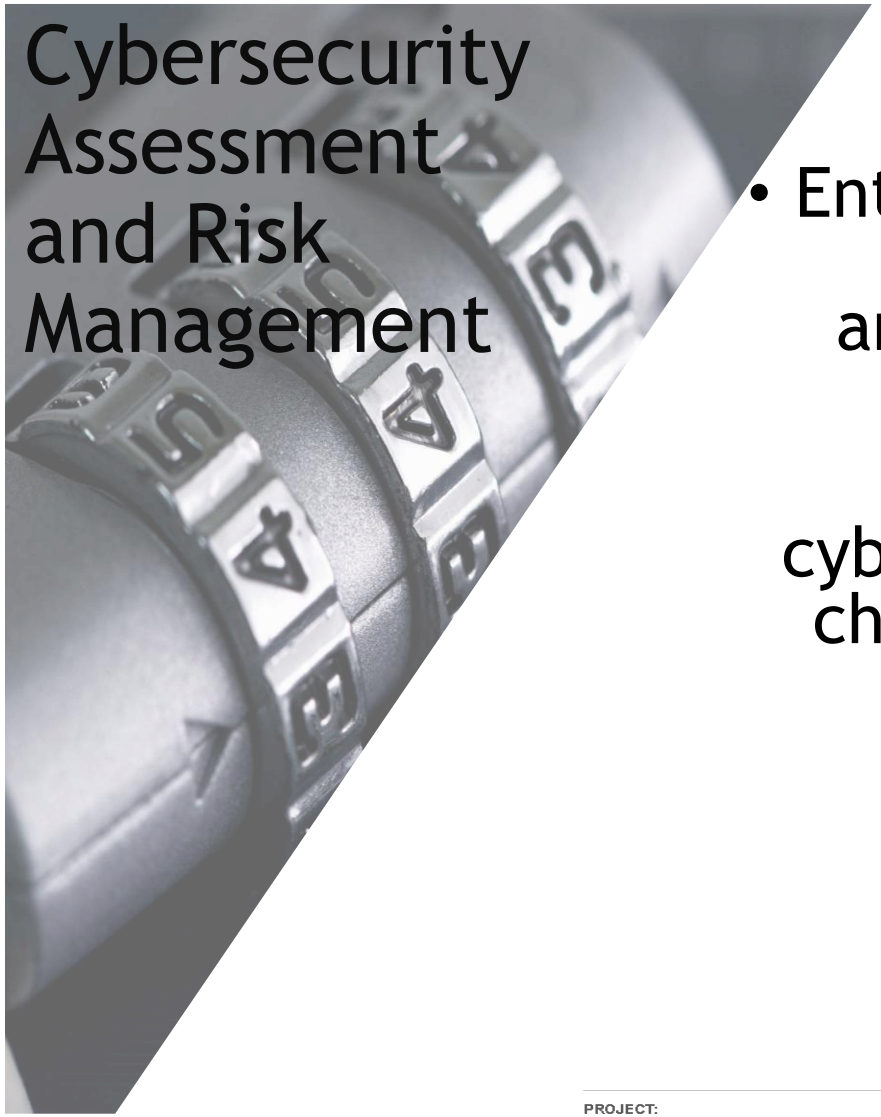
PROJECT:
101128047 – INFORB – DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE
Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

Awareness and Training Programs

- Awareness Workshops: We conduct workshops for food sector entities and the public to raise awareness about cybersecurity risks and best practices
- Training Schemes: We develop comprehensive training schemes for entity management, equipping them with the skills needed to oversee cybersecurity effectively
- Cybersecurity Personnel Training: Specialized training sessions are provided to personnel responsible for cybersecurity within food entities, enhancing their ability to protect critical systems

INFORB
PROJECT:
101128047 – INFORB – DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE
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.

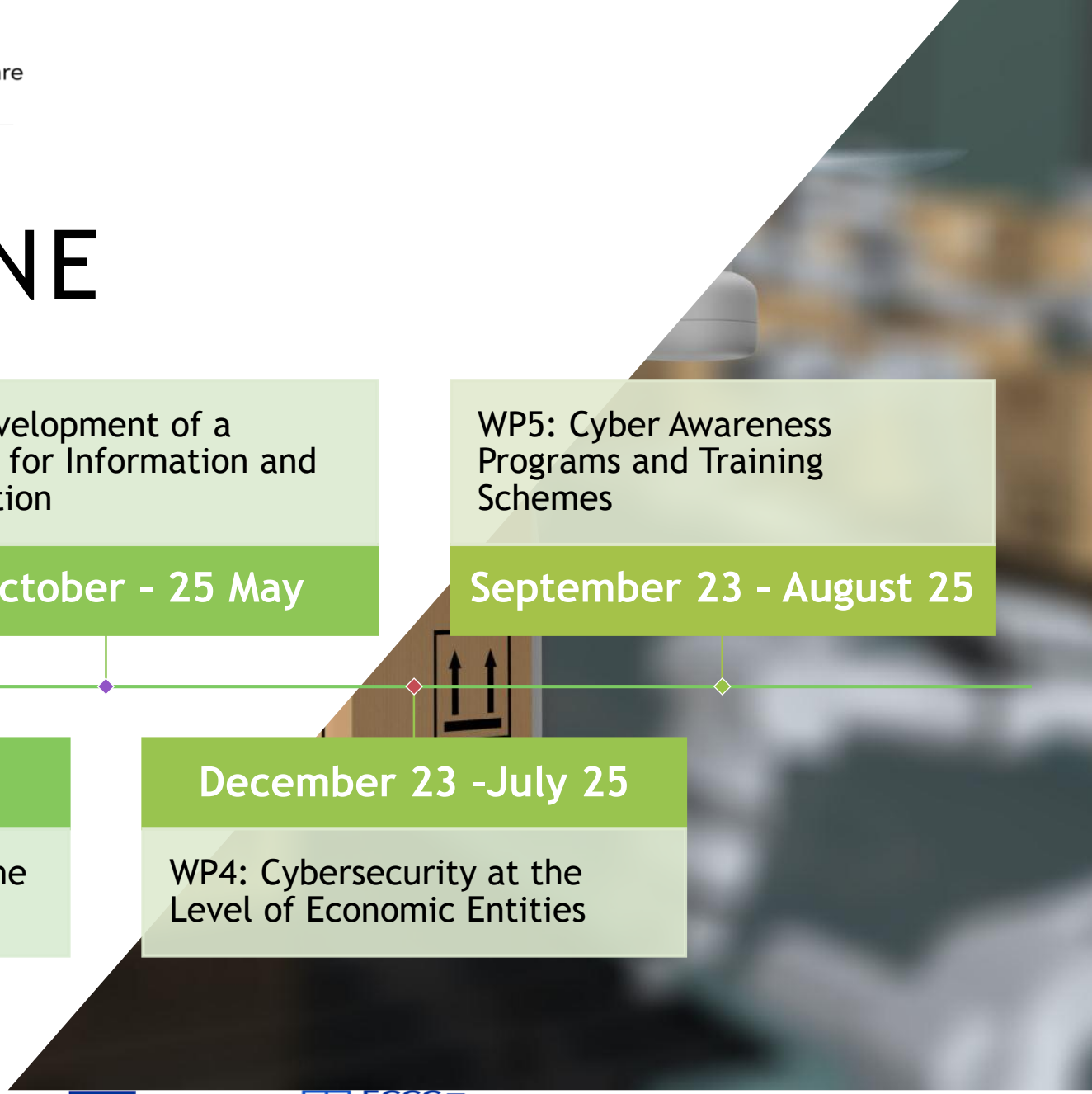
Cybersecurity Assessment and Risk Management



- Entity-Level Assessment: We conduct surveys on food sector entities' network security, analyzing their current cybersecurity status and vulnerabilities
- Supply Chain Risk Management: Unique cybersecurity risks related to the food supply chain are identified, assessed, and managed
- Risk Minimization: We develop a comprehensive cybersecurity risk management manual specific to the food supply chain

PROJECT:
101128047 – INFORB – DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE
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.

PROJECT TIMELINE



WP1: Project Management and Coordination

September 23 – August 25

WP3: Development of a Platform for Information and Cooperation

23 October – 25 May

WP5: Cyber Awareness Programs and Training Schemes

September 23 – August 25

October 23 – July 25

WP2: Economic Entities in the Food Sector

December 23 –July 25

WP4: Cybersecurity at the Level of Economic Entities

PROJECT:
101128047 – INFORB – DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE
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.

Thank you!

Info:
https://egov.government.bg/wps/portal/ministry-meu/home/programs.projects/projects-progress/digitaleurope

Contact: dmis@egov.government.bg

PROJECT:
101128047 – INFORB – DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE
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.