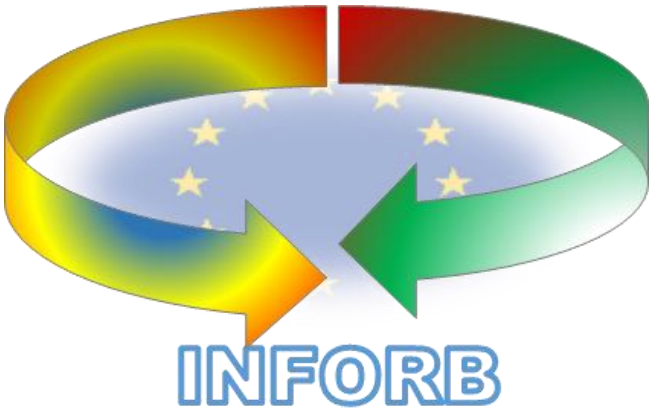

GOOD PRACTICE GUIDE REGARDING THE IMPLEMENTATION OF THE NIS 2 DIRECTIVE AT THE LEVEL FOOD SECTOR

DELIVERABLE D2.2

Version 1.0

31.10.2024

SUMMARY

This *'Guide to good practice on the implementation of the NIS 2 Directive in the food sector'* provides several recommendations and solutions to ensure and strengthen the security of network and information systems, with a focus on the key stages of the implementation process. The NIS 2 Directive, adopted at European Union level, lays down cybersecurity requirements for critical infrastructures, including the food sector, which face increased risks in the context of digitalisation and interconnectivity, and which must take rigorous measures to protect against cyber threats.

The guide includes detailed steps on the 'identification, classification and record-keeping' of food business entities, which are essential for the initial preparation of the implementation of the NIS 2 Directive. The steps are fundamental to understand the vulnerabilities specific to the food sector and to establish a coherent plan of cybersecurity measures across the sector. It also provides good practices for identifying stakeholders in cyber threat management, incident prevention and food supply chain protection.

By disseminating this guide, we aim to support all actors in the food sector in adopting effective cybersecurity measures, ensuring compliance with the NIS 2 Directive and reducing digital vulnerabilities.

PROJECT:

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

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Document control information

Settings	Value
Document title:	Good practice guide regarding the implementation of the NIS 2 Directive at the level of the food sector
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:	Gabriel Hîmpă; Gergana Rakova
Deliverable identifier:	D2.2
Due date of delivery:	31.10.2024
Date of delivery:	31.10.2024
Project Manager (PM):	Constantin Călin
Document version:	V1.0
Sensitivity:	PU-Public
Date:	31.10.2024

Evaluators and document evaluators

Name	Rol	Action	Date
Gabriel Hîmpă	WP2 Leader	Draft document created	15.09.2024
Gabriel Hîmpă	WP2 Leader	Original version (DNSC)	08.10.2024
Mihai Guranda	Project Assistant Manager	Quality assurance version	31.10.2024
Constantin Călin	Project Manager	Final document assumed and delivered	31.10.2024

Document history

Revision	Date	Created by	Brief description of the changes
V0	15.09.2024	WP2 Leader	Document creat
V0.1	30.10.2024	WP2 Leader	Correction of the updated information document
V1.0	31.10.2024	WP2 Leader	Updating the document

Table of contents

INTRODUCTION

The "*Guide to Good Practice on the Implementation of the NIS 2 Directive in the Food Sector*", hereinafter referred to as *"Guide* or *Guide to Good Practices"*, was developed within the framework of the project "Implementation of the NIS Directive in the food production, processing and distribution sector in Romania and Bulgaria" (INFORB) co-financed by the European Commission, which aims at ensuring cybersecurity, managing supply chain-specific cybersecurity risks, identifying essential and important entities in a sector of critical importance, namely *"Food production, processing and distribution" (PPDA)*, a sector newly 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, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

The main purpose of the project is to identify economic entities and classify them into essential and important entities in a sector of critical importance, to assess and ensure cybersecurity, including the supply chain, namely for "the food production, processing and distribution" sector ("the food sector").

The Guide is an important tool for food businesses to strengthen and improve their cybersecurity capabilities to better manage risks and threats in the digital environment in which they operate**.**

Purpose

The *Guide to Good Practices* is designed to provide clear, detailed and structured guidance to ensure compliance with the requirements of the NIS 2 Directive. The main purpose of the guide is to support food business enterprises in correctly identifying and classifying into essential and/or important entities and to facilitate the efficient and uniform implementation of cybersecurity measures in the food sector, thereby ensuring adequate protection of network and information systems critical to the safety and integrity of the food chain, as well as adequate documentation of the processes necessary to ensure transparency and accountability in cybersecurity management.

Objectives

Ensuring compliance with the NIS 2 Directive

A first objective of the implementation of the NIS 2 Directive is **to ensure compliance with it** in the food sector by (1) promoting and ensuring robust and efficient cybersecurity in the critical infrastructures of entities in this sector; (2) providing a clear framework for understanding the requirements of the NIS 2 Directive and how they apply specifically to the food sector; and (3) supporting essential and important entities in the food sector in implementing the measures necessary to comply with the Directive, reducing the risk of sanctions and penalties.

Critical infrastructure protection

A second important objective is **to identify and protect critical infrastructures** that have a significant impact on cybersecurity and the proper functioning of essential services. These may include data processing systems, distribution networks, production management systems, etc.

Implementation of cybersecurity measures

In the same context, the adoption of standards and recommended practices involving the **implementation of cybersecurity measures** as required by the NIS 2 Directive and relevant national and international standards is another important objective. These measures may include data encryption, access management, continuous monitoring of networks and systems, and rapid response to security incidents.

Cybersecurity risk assessment and management

Another important objective is **to assess and manage cybersecurity risks.** This process involves identifying threats, assessing vulnerabilities and taking preventive and corrective measures to reduce risks to an acceptable level.

Business Continuity Planning

In order to ensure operational continuity, **business continuity planning is** an essential objective achievable through **(1) the development** and (2) the implementation of business continuity plans to ensure the ability to deal with and quickly return to normality in the event of a cybersecurity incident or other unforeseen events.

Employee awareness and training

Cybersecurity culture is also an important objective achievable at the level of each business through **employee awareness and training (continuous processes)**, achieved through awareness sessions and the active involvement of employees in the protection of data, information and network and information systems.

Monitoring and auditing of network and information systems

Monitoring and auditing of network and information systems is a last important objective of the implementation of the NIS 2 Directive in the food sector. The process can be achieved through (1) the implementation of continuous monitoring mechanisms of network and information systems for the early detection of potential cybersecurity threats or incidents, and (2) regular (regular) auditing of network and information systems to ensure compliance with applicable cybersecurity policies and standards.

SECTION 1. IDENTIFICATION OF ENTITIES

In this section, the focus is on supporting food business enterprises in the identification process as entities to which the NIS 2 Directive applies. Proper identification of entities is important to ensure that they meet their compliance obligations and manage cyber risks effectively according to their sector membership and the technological complexity of the network and information systems underpinning the provision of services.

STAGES OF IDENTIFICATION OF ENTITIES TO WHICH NIS 2 DIRECTIVE APPLIES

Stage 1. Membership in the food sector

The procedure involves assessing the main activities of the business to determine whether the activities are related to the food sector. Activities may include production, processing, distribution, sale or serving of food. The first stage in the identification process is an essential one in determining whether the NIS 2 Directive applies to that entity.

↳ The steps and criteria necessary for effective implementation of this stage:

1.1. Identification of core activities

1.1.1. Definition of food activities

- **Production:** Activities involved in the cultivation, harvesting and rearing of food raw materials, such as agriculture, fisheries and livestock farming.
- **Processing:** Transformation of food raw materials into finished products, including activities such as meat processing, dairy production, and preservation of vegetables and fruits.
- **Distribution:** Transport and storage of food products to points of sale or other intermediaries in the supply chain.
- **Sale and food services:** Retail and wholesale trade of food products as well as catering services, including restaurants, canteens and catering.

1.1.2. Verification of activities

- **Analysis of internal documentation:** Review the entity's internal documents, such as activity reports, financial statements, websites and marketing materials to identify relevant activities.
- **Interviews and inspections:** Conduct interviews with key personnel and on-site inspections to confirm the activities carried out.

1.2. Verification of the sector of activity

1.2.1. NACE classification

- **Relevant NACE codes:** Identification and use of NACE codes that are relevant to activities in the food sector. NACE codes – specific to the food sector – include the divisions:
  - ✓ **01** – Agriculture, hunting and related services.
  - ✓ **10** – Food industry (exceptions: tobacco and animal feed).
  - ✓ **11** – Manufacture of beverages.

- ✓ **46** – Wholesale trade, except of motor vehicles and motorcycles (relevant groups and classes).
- ✓ **52** - Storage and ancillary activities for transport (Group 521 – Storage).
- ✓ **55** - Hotels and other accommodation facilities.
- ✓ **56** - Restaurants and other food service activities.

1.2.2. Verification of CAEN registration

- ➲ **Official documents:** Verification of the entity's official records in the business register and other government databases to confirm the CAEN codes under which the entity is registered.

1.3. Licenses and authorisations

1.3.1. Verification of compulsory licenses

- ➲ **Veterinary authorisations:** Verification of the existence of the necessary veterinary authorisations for carrying out food activities.
- ➲ **Food safety certifications:** Verification of food safety certifications, such as ISO 22000 (Food Safety ManagementSystem - international standard for food safety management systems),HACCP (HazardAnalysis and Critical Control Point Control - is a systematic method for identifying, assessing and controlling food safety risks, is focused on preventing food contamination instead of detecting it in finished products), BRC (BritishRetail Consortium - is to ensure that suppliers meet specific food safety, hygiene, quality control and other relevant standards) or other recognised standards.

1.3.2. Regulatory compliance

- ➲ **Compliance analysis:** Assessment of the compliance of the entity with national and European legislation on food safety and food hygiene.

1.4. Product Portfolio Assessment

1.4.1. Product/Service Analysis

- ➲ **Product categories:** Classification of the goods or services provided by the entity to determine whether they are food-related or directly related to the food industry.
- ➲ **Importance and place of the entity in the food sector:** Assess the position of the entity in the food value chain to understand its role and impact in the sector.

1.4.2. Marketing Information

- ➲ **Promotional materials:** Review promotional material and publicly available information to confirm activities related to the food sector.

1.5. Relations with third parties

1.5.1. Evaluation of collaborations

- ➲ **Partners and suppliers:** Identifying collaborations and business relationships with other organizations in the food sector, such as raw materials suppliers, distributors and main customers.
- ➲ **Contracts and agreements:** Review contracts and agreements to confirm the nature of activities and membership of the food sector.

1.5.2. Feedback from partners

- **References:** Require references and feedback from business partners to verify the entity's activities and reputation in the food sector.

1.6. Conclusions and documentation

1.6.1. Evaluation report

- **Documentation:** Preparation of a detailed report summarising the evaluation process, the criteria used and the conclusions on the entity's membership in the food sector.
- **Justifications:** Provide justifications and records supporting the conclusions of the report.

1.6.2. Internal approval

- **Review and approval:** Review of the report by the compliance team or management of the entity and its approval for use in the later stages of the NIS 2 compliance process.

This detailed step ensures that only businesses with relevant activities in the food sector are identified and considered for compliance with the NIS 2 Directive, establishing a sound basis for further assessments and classifications.

Stage 2. Fulfilment of special criteria

The stage involves assessing the entities identified in the previous step to verify whether they meet the specific criteria set out in the NIS 2 Directive. These criteria are essential to determine whether a food business entity must comply with the requirements of the Directive.

↳ The steps and criteria necessary for effective implementation of this stage:

2.1. Safety and security impact assessment

2.1.1. Impact on food security

- **Risk analysis**: Assessment of risks associated with the activities of the entity that could affect food security, including cyber risks that could disrupt the supply chain or food production.
- **Incident scenarios:** Development and assessment of possible cyber incident scenarios and their impact on food safety.

2.1.2. Impact on public health

- **Hazard assessment:** Analysis of potential dangers to public health caused by disruptions in the supply chain or compromising the integrity of food products due to cyber-attacks.

2.2. Assessment of critical infrastructure dependency

2.2.1. Related critical infrastructures

- **Identification of connections:** Determining whether the entity has critical interdependencies with other critical infrastructure such as energy, transport, water and telecommunications networks.
- **Essential role:** Assess the essential role of the entity in maintaining the functioning of these critical infrastructures, in the context of food security.

2.2.2. Vulnerability assessment

- **Identification of vulnerabilities:** Analysis of vulnerabilities of critical infrastructures on which the entity depends and the potential knock-on effects of a cyber incident.
- **Protective measures:** Verify the safeguards in place to secure these critical interdependencies and prevent spill-over effects of cyber incidents.

2.3. Economic and social importance

2.3.1. Economic impact

- **Contribution to the economy:** Assessment of the entity's economic contribution to the food sector and the national economy, including aspects such as turnover, number of employees and role in exports/imports.
- **Financial impact:** Analysis of the potential financial impact of a cyber incident on the entity and the food sector as a whole.

2.3.2. Social impact

- **Role in the community:** Assessment of the social importance of the entity, including the provision of employment, community support and other social contributions.
- **Social risks:** Identifying social risks associated with disruptions to the entity's activities caused by cyber incidents, such as food shortages or job losses.

2.4. Compliance with security standards

2.4.1. Certifications and accreditations

- **Cybersecurity certifications:** Verification of international and national cybersecurity certifications, such as ISO/IEC 27001.
- **Compliance with standards:** Assessment of the entity's compliance with cybersecurity standards relevant to the food sector.

2.4.2. Security policies and procedures

- **Security policies:** Review the cybersecurity policies implemented by the entity to ensure adequate protection of network and information systems.
- **Response procedures:** Evaluate incident response procedures and business continuity plans to manage and minimize the effects of cyber incidents.

2.5. Assessment of incident response capability

2.5.1. Equipment and technologies

- **Technological infrastructure:** Assessment of the technological infrastructure used to detect, prevent and respond to cyber incidents.
- **Monitoring systems:** Check monitoring systems and the ability to quickly detect and respond effectively to incidents.

2.5.2. Human resources and training

- **Specialised staff:** Assessing the availability and skills of cybersecurity personnel.
- **Training programs:** Verify the existence of continuous training programs for staff to maintain and improve incident response capacities.

2.6. Evaluation and documentation report

2.6.1. Centralisation of results

- **Detailed report:** Preparation of a detailed report summarising the results of the assessment of the special criteria, including all necessary evidence and justifications.
  - ✓ **Conclusions:** Presentation of conclusions on the fulfilment of the special criteria and qualification of the entity for compliance with the NIS 2 Directive.

2.6.2. Documentation and archiving

- **Record keeping:** Maintain a complete and well-organised record of all documents and information used in the evaluation process.
- **Periodic review:** Establish a process of periodic review of documentation to reflect necessary changes and updates.

These intermediate steps guarantee a complete and detailed assessment of food business entities, facilitating the correct identification of those who need to comply with the NIS 2 Directive. It establishes an effective framework for protecting critical infrastructure and ensuring food security at national and European levels.

Stage 3. Size of the economic entity

This stage involves assessing the economic size of food businesses to determine their eligibility under the NIS 2 Directive. The economic dimension is a key criterion in determining the impact and relevance of entities in the food sector, helping to ensure compliance with cybersecurity requirements.

Size represented by thresholds that are calculated on the basis of figures for the whole legal entity (including all its activities, even outside the EU), consolidated in proportion to the figures of partner or linked enterprises.

For more details on how to calculate these thresholds, see Annex I to Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, the guide published by the European Commission or its online tool.

Useful links to determine the size of the economic enterprise:

- European Commission Recommendation 2003/361/EC of 6 May 2003: https://eur-lex.europa.eu/eli/reco/2003/361/oj
- "User's Guide to the SME Definition" (European Commission): https://op.europa.eu/en/publication-detail/-/publication/756d9260-ee54-11ea-991b-01aa75ed71a1
- SME Self-AssessmentTool (European Commission): https://ec.europa.eu/growth/tools-databases/SME-Wizard.

↳ The steps and criteria necessary for effective implementation of this stage:

3.1. Assessment of the economic dimension

3.1.1. Size criteria

- **Number of employees:** Assessment of the average number of employees during a financial year. This is a key indicator of the economic size of the entity.
- **Turnover:** Analysis of annual turnover, which reflects the total revenue generated by the entity in a financial year.
- **Total assets:** Measurement of the total value of assets held by the entity, including land, buildings, equipment, and other property.

3.1.2. Size thresholds

- **Micro-enterprises:** Entities with fewer than 10 employees and an annual turnover or total assets of less than EUR 2 million.
- **Small businesses:** Entities with fewer than 50 employees and an annual turnover or total assets of less than EUR 10 million.
- **Medium-sized enterprises:** Entities with fewer than 250 employees and an annual turnover of less than EUR 50 million or total assets of less than EUR 43 million.
- **Large companies:** Entities exceeding the limits set for small and medium-sized enterprises.

3.2. Assessment methodology

3.2.1. Collection of financial data

- **Data sources:** Use of annual financial reports, balance sheets and other relevant financial documents to collect data necessary to assess the economic size.
- **Historical data:** Collection and analysis of financial data over several years to identify trends and ensure accuracy of the valuation.

3.2.2. Data validation

- **Internal audits:** Carrying out internal audits to validate the accuracy of the financial data collected.
- **External checks:** Using the services of external auditors to verify the compliance of financial data with accounting standards and legal regulations.

3.3. Analysis and interpretation of data[1]

3.3.1. Calculation of key indicators

- **Average number of employees:** Calculation of the annual average number of employees based on monthly reports.
- **Turnover:** Calculation of annual turnover based on total revenue generated from the sale of products and services.
- **Total assets:** Determine the total value of assets by summing up the carrying amount of all assets held.

3.3.2. Comparison with size thresholds

- **Categorisation:** Comparison of the key indicators calculated with the size thresholds set for micro, small, medium-sized and large enterprises to qualify the entity in the appropriate category.

3.4. Assessment of structural complexity

3.4.1. Analysis of organisational structure

- **Management structure:** Assess the management structure and hierarchical levels within the entity to determine organisational complexity.

[1] To work out the data to be considered and assessed against the thresholds, an enterprise must first establish whether it is: (a) an autonomous enterprise (by far the most common category); (b) a partner enterprise; or (c) a linked enterprise.
Depending on the situation, an enterprise may have to take into account: (1) only its own data; (2) a proportion of the data in case of a partner enterprise; or (3) all the data of any enterprise considered linked to it.

- **Divisions and departments:** Analyze the number and functions of divisions and departments in the entity to assess operational complexity.

3.4.2. Operational complexity assessment

- **Supply chain:** Analysis of the complexity of the supply chain and the number of partners and suppliers involved.
- **Technological processes:** Assessment of the complexity of technological processes used in the production, processing and distribution of food products.

3.5. Documentation and reporting

3.5.1. Evaluation report

- **Detailed documentation:** Preparation of a detailed report containing the valuation methodology, the data collected, the analyses carried out and the conclusions on the economic size of the entity.
- **Recommendations**: Provide recommendations for necessary compliance measures depending on the economic size category the entity falls into.

3.5.2. Review and approval

- **Internal review:** Review of the report by the compliance team and management of the entity to ensure accuracy and correctness of the assessment.
- **Final approval:** Approval of the report by the management of the entity and its archiving for future reference and use in the later stages of the NIS 2 compliance process.

This detailed stage of assessing the economic size of entities ensures a clear and precise understanding of their importance and impact in the food sector. This facilitates the correct and efficient application of the NIS 2 Directive, contributing to the cybersecurity and resilience of the food sector.

Stage 4. Qualification as an entity to which the NIS 2 Directive applies

The stage provides a clear and detailed structure for the process of identifying the entities to which the NIS 2 Directive is applicable in the food sector, where they are correctly identified and that they are subject to the appropriate provisions for managing cybersecurity effectively.

It is important that this stage is carefully followed and well documented to ensure compliance and effectiveness in managing cyber risks.

↳ The steps and criteria necessary for effective implementation of this stage:

4.1. Summary of previous evaluations

4.1.1. Integration of results

- **Membership in the food sector:** Establishment that the entity meets the food sector membership criteria based on NACE codes and core activities.
- **Fulfilment of the special criteria:** Confirmation that the entity meets the special criteria for impact on food security, public health, critical infrastructures, and compliance with cybersecurity standards.
- **Economic dimension:** Verification that the entity falls within the economic size thresholds relevant for the NIS 2 Directive (micro, small, medium-sized or large enterprises).

4.1.2. Integrated assessment

- **Integrated analysis:** Combining the results of previous assessments into an integrated report that concludes the entity's status at each of the previous stages.
- **Overall compliance:** Assessment of the entity's overall compliance against multiple criteria to determine whether it needs to comply with the NIS 2 Directive.

4.2. Assessment of potential impact

4.2.1. Impact on national security

- **Role in national security:** Assessment of the role of the entity in maintaining food security and other critical infrastructure at national level.
- **Risk potential:** Determine the potential risk that the entity may pose to national security in the event of cyber incidents.

4.2.2. Impact on network and information systems

- **Technological complexity:** Assessment of the complexity and interconnectivity of the network and information systems used by the entity.
- **Critical vulnerabilities:** Identification of critical vulnerabilities and potentially exploitable access points in the entity's network and information systems.

4.3. Compliance with legal and regulatory requirements

4.3.1. Cybersecurity requirements

- **Security standards:** Verification of the entity's compliance with international and national cybersecurity standards, such as ISO/IEC 27001.
- **Policies and procedures:** Assess the existence and effectiveness of cybersecurity policies and procedures implemented by the entity.

4.3.2. Reporting requirements

- **Reporting obligations:** Verification of the entity's compliance with the reporting obligations imposed by the NIS 2 Directive, including notification of cybersecurity incidents.
- **Transparency and accountability:** Assess the level of transparency and accountability of the entity in reporting and managing security incidents.

4.4. Final determination of the qualification

4.4.1. Decision analysis

- **Qualification criteria:** Apply a final set of decision-making criteria to determine whether the entity needs to comply with the NIS 2 Directive.
- **Compliance score:** Assign a compliance score based on the results of previous assessments and final decision criteria.

4.4.2. Compliance decision

- **Classification of the entity:** Classification of the entity as subject or not subject to the requirements of the NIS 2 Directive.

- **Communication of the decision:** Communication of the final decision to the entity, including a detailed justification of the conclusions and the next steps required for compliance.

4.5. Continuous documentation and monitoring

4.5.1. Final qualification report

- **Detailed documentation:** Preparation of a final report documenting the entire assessment and qualification process, including all relevant steps and conclusions.
- **Archiving documents:** Archiving the report and all supporting documents for future references and for possible inspections or audits.

4.5.2. Continuous monitoring

- **Periodic reviews:** Establish a timetable for regular reviews to update assessments and ensure continued compliance with the NIS 2 Directive.
- **Updating information:** Maintain up-to-date information about the entity's economic size, organisational structure and compliance.

This final stage of classification ensures that all relevant food business entities are identified correctly and as required by the NIS 2 Directive. The detailed assessment and qualification process contributes to the security and resilience of critical infrastructures, thereby safeguarding food security and public health.

SECTION 2. CLASSIFICATION OF ENTITIES

STAGES OF CLASSIFICATION OF ENTITIES BY IMPORTANCE

Stage 1. Assessment of essential entity status

Criteria and assessment process for determining essential entities:

(1) This step focuses on the assessment of entities to determine whether they can be classified as essential entities within the food sector under the NIS 2 Directive.

(2) Essential entities play an important role in maintaining food security and public health, as well as in the continuous functioning of critical infrastructures.

↳ The steps and criteria necessary for effective implementation of this stage:

1.1. Identification of evaluation criteria

1.1.1. Importance

- **Role in the supply chain:** Assess the position of the entity in the food supply chain and its importance in the continuous supply of essential food products.
- **Critical interdependencies:** Identify critical interdependencies with other entities and infrastructures that could affect the continued functioning of the food sector.

1.1.2. Potential impact of incidents

- **Food security:** Assessing the potential impact of a cyber incident on food security, including food **availability** and safety.
- **Public health:** Determining the impact on public health in the event of an incident affecting the quality or availability of food.

1.1.3. Size and capacity

- **Production and distribution capacity:** Assessment of the production and distribution capacity of the entity and its role in ensuring food supply on a national or regional scale.
- **Number of beneficiaries:** Analysis of the number of consumers or other entities dependent on the products and services provided by the entity.

1.2. Assessment methodology

1.2.1. Data collection and analysis

- **Data sources:** Use internal reports, market data, and information from relevant authorities to collect data about the entity's systemic importance and potential impact.
- **Interviews and consultations:** Conduct interviews and consultations with food experts, regulators and other stakeholders to gain further insights.

1.2.2. Risk assessment

- **Analysis of incident scenarios:** Risk assessment through analysis of hypothetical cyber incident scenarios and their impact on entity functioning and food security.

- **Mitigation measures:** Identify the entity's existing measures and response capacities to manage and reduce cyber risks.

1.3. Determination of essential entity status

1.3.1. Setting assessment thresholds

- **Qualitative and quantitative criteria:** Use a combined set of qualitative (e.g. strategic importance, interdependence) and quantitative (e.g. production capacity, number of beneficiaries) criteria to assess the importance of the entity.
- **Scores and indicators:** Assign scores and indicators for each assessment criterion to facilitate comparison and classification of entities.

1.3.2. Final classification

- **Classification decision:** Classification of entities that meet or exceed the thresholds established as essential entities. This involves analysing the scores and indicators obtained and comparing them with the reference thresholds.
- **Documentation of the decision:** Elaboration of a detailed report documenting the evaluation process, the criteria used, the assigned scores and the conclusions on the classification of entities.

1.4. Communication and monitoring

1.4.1. Information to entities

- **Communication of results:** Communicating the results of the assessment and classification decision to those entities, including the detailed justification for classification as an essential entity;
- **Compliance obligations:** Informing entities of the additional compliance obligations and requirements imposed by the classification as an essential entity.

1.4.2. Continuous monitoring

- **Periodic reviews:** Establish a program of regular reviews to reassess the classification of entities and ensure continued compliance with the NIS 2 Directive.
- **Updating information:** Updating information about entities based on changes in production capacity, organizational structure, and other relevant aspects that may influence their classification.

This detailed essential entity assessment step ensures the correct identification of entities that play a key role in the food sector and need to comply with the requirements of the NIS 2 Directive to maintain cybersecurity and the resilience of critical infrastructures.

Stage 2. Assessment of the quality of important entity

The phase focuses on the identification and assessment of entities that, although not classified as essential, play a significant role in the food sector and must comply with the requirements of the NIS2 Directive. Important entities are those that contribute substantially to the normal functioning and resilience of the food sector, having a considerable impact on the supply chain and food security.

↳ The steps and criteria necessary for effective implementation of this stage:

2.1. Identification of evaluation criteria

2.1.1. Importance in the supply chain

- **Supply contribution:** Assessment of the entity's contribution to the food supply, including its role in production, processing, distribution and sale.
- **Interdependencies in the supply chain:** Identifying interdependencies with other entities and the potential impact on the supply chain in case of incidents.

2.1.2. Impact on consumers

- **Geographical spread:** Assessing the geographical distribution of the entity's operations and the number of consumers served.
- **Product diversity:** Analysis of the diversity and importance of food products provided by the entity in the diet and nutrition of the population.

2.1.3. Incident response capability

- **Operational resilience:** Assess the entity's ability to respond and recover quickly in the event of cyber incidents or other disruptions.
- **Continuity plans:** Verifying the existence and effectiveness of business continuity plans and risk mitigation measures.

2.2. Assessment methodology

2.2.1. Data collection and analysis

- **Data sources:** Use data from activity reports, information from relevant authorities and market studies to collect the information necessary for the assessment.
- **Stakeholder consultations:** Organise consultations with food industry representatives, regulators and experts to gain a comprehensive view of the importance of the entity.

2.2.2. Risk and vulnerability assessment

- **Risk analysis:** Assessing the specific risks and vulnerabilities that may affect the entity and, implicitly, the food supply chain.
- **Impact of incidents:** Analysis of the potential impact of cyber incidents on the operations of the entity and on final consumers.

2.3. Determination of the quality of important entity

2.3.1. Setting assessment thresholds:

- **Qualitative and quantitative criteria:** Defining qualitative (e.g. impact on the supply chain, number of customers served) and quantitative (e.g. production capacity, turnover) criteria for assessing significance.
- **Performance indicators:** Assign performance indicators for each criterion to facilitate the assessment and comparison of entities.

2.3.2. Final classification

- **Analysis of scores:** Calculation and analysis of scores based on the criteria established to determine whether the entity qualifies as an important entity.

- **Documentation of the process:** Elaboration of a detailed report documenting the evaluation process, the criteria used, the scores obtained and the conclusions on the classification of entities.

2.4. Communication and monitoring

2.4.1. Information to entities

- **Communication of the decision:** Communicating the results of the assessment and classification decision to those entities, including detailed justification for classification as an important entity.
- **Compliance obligations:** Informing entities of the additional compliance obligations and requirements imposed by the classification as an important entity.

2.4.2. Continuous monitoring

- **Periodic reviews:** Establish a timetable for regular reviews to reassess the classification of entities and ensure continued compliance with the NIS 2 Directive.
- **Updating information:** Maintain up-to-date information about the economic size, organisational structure and responsiveness of the entity.

This detailed step of the important entity assessment ensures that all relevant food business entities are correctly identified and appropriately classified to comply with the requirements of the NIS 2 Directive. The process contributes to the security and resilience of the food sector, thereby protecting consumers and supply chains from cyber threats.

Stage 3. Identification as a non-critical entity

The stage focuses on identifying entities that, although part of the food sector, are not considered essential or important according to the criteria of the NIS 2 Directive. Non-critical entities have less impact on food security and the supply chain, with less exposure and risk in the event of a cyber incident.

↳ The steps and criteria necessary for effective implementation of this stage:

3.1. Identification of evaluation criteria

3.1.1. Economic size and capacity

- **Limited production capacity**: Assessment of the size of the production capacity of the entity where production does not have a significant impact on national or regional level.
- **Turnover:** Verification of annual turnover, which is relatively low compared to essential and important entities.

3.1.2. Low impact on the supply chain

- **Limited geographical spread:** entities that operate in a restricted geographical area and do not have a significant influence on the national or regional supply chain.
- **Number of beneficiaries:** the low number of consumers or entities dependent on the products and services provided.

3.1.3. Resilience of systems

- **Support systems:** entities that have surplus information in their operating and support systems, reducing the risk of impact in the event of an incident.

- **Recovery capacity:** assessing the entity's ability to recover quickly in the event of disruption with minimal impact on consumers and the supply chain.

3.2. Assessment methodology

3.2.1. Data collection and analysis

- **Data sources:** using data from financial reports, risk assessments and information from regulators to collect information about the size and capacity of the entity.
- **Stakeholder consultations:** carrying out consultations with entities, experts and authorities to validate the information collected and obtain further insights.

3.2.2. Risk and vulnerability assessment

- **Specific risk analysis:** assessing the specific risks associated with the entity's operations, taking into account the limited impact on food security and the supply chain.
- **Impact of incidents:** analysis of the potential impact of incidents on the entity's operations, focusing on local risks and the minimum impact on consumers.

3.3. Determination of the quality of non-critical entity

3.3.1. Setting assessment thresholds

- **Qualitative and quantitative criteria:** Definition of qualitative (e.g. local importance, system capabilities -implementation of back-up measures or duplication of components or functions of a system to ensure continuity of operation in case of failures or errors) and quantitative (e.g. production capacity, turnover) criteria for assessing low importance.
- **Performance indicators:** Assign performance indicators for each criterion to facilitate the assessment and comparison of entities.

3.3.2. Final classification

- **Analysis of scores:** Calculation and analysis of scores based on the criteria established to determine whether the entity qualifies as a non-critical entity.
- **Documentation of the process:** Elaboration of a detailed report documenting the evaluation process, the criteria used, the scores obtained and the conclusions on the classification of entities.

3.4. Communication and monitoring

3.4.1. Information to entities

- **Communication of the decision:** Communicating the results of the assessment and classification decision to those entities, including detailed justification for classification as a non-critical entity.
- **Compliance obligations:** Informing entities about additional obligations and requirements, even if they are minimal compared to those for essential and important entities.

3.4.2. Continuous monitoring

- **Periodic reviews:** Establish a timetable for regular reviews to reassess the classification of entities and ensure continued compliance with the NIS 2 Directive.
- **Updating information:** Maintain up-to-date information about the economic size, organisational structure and responsiveness of the entity.

Through this detailed non-critical entity assessment step, it ensures that all food business entities are correctly classified, thus contributing to effective risk management and cybersecurity protection, even for low-impact entities. This detailed process helps clarify responsibilities and allocate security resources in a manner commensurate with the importance of entities in the food sector.

Stage 4. Final classification of entities

The stage is the culmination of the process of assessing and classifying food business entities under the NIS 2 Directive. The final classification of entities ensures a clear and detailed understanding of the importance of each entity and contributes to the implementation of cybersecurity measures commensurate with their role and impact.

↳ The steps and criteria necessary for effective implementation of this stage:

4.1. Summary and analysis of evaluation data

4.1.1. Centralisation of interim results

- **Results of previous steps:** Collecting and reviewing results from previous stages of the evaluation process (essential, important, non-critical entities).
- **Comparison of scores and indicators:** Comparison of scores and indicators obtained by entities based on the criteria established at each stage to ensure consistency and accuracy of assessments.

4.1.2. Collective analysis

- **Cumulative impact:** Assess the cumulative impact of entities on the food sector, considering interdependencies and redundancies in the supply chain.
- **Identification of key entities:** Identifying which entities, while individually classifiable as non-critical or important, together play a key role in ensuring food security.

4.2. Process validation and verification

4.2.1. Consistency check

- **Internal review:** Carrying out an internal review to verify the consistency and correctness of the evaluation and classification process, ensuring that all criteria have been applied uniformly.
- **External audit:** Where necessary, request an external audit to validate the process and the results achieved, providing an objective and independent perspective.

4.2.2. Adjustment of valuations

- **Feedback and reviews:** Integrate feedback from stakeholders, experts and authorities, and adjust assessments where necessary to reflect changes or comments received.
- **Data update:** Updating valuation data in the light of recent changes in the economic dimension, production capacity and other relevant variables.

4.3. Determination of the final classification

4.3.1. Setting definitive thresholds

- **Qualitative and quantitative criteria:** Definition and final application of qualitative and quantitative criteria for each category (essential, important, non-critical), ensuring that thresholds are clear and justified.
- **Baseline assessments:** Use established benchmarks to compare and classify entities definitively.

4.3.2. Preparation of the final report

- **Documentation of the process:** Produce a detailed report documenting the entire evaluation and classification process, including the methodology, criteria used, results achieved and final decisions.
- **Justification of decisions:** Provide a clear and detailed justification for the classification of each entity, based on the data and analyses performed.

4.4. Communication and implementation

4.4.1. Classification communication

- **Information to entities:** Formal communication of the final classification to each assessed entity, together with a detailed report explaining the results and compliance obligations.
- **Dissemination of information:** Distribute relevant information to regulators and other stakeholders to ensure transparency and accountability.

4.4.2. Implementation of compliance requirements

- **Compliance guides:** Provide guidance and recommendations to entities on the necessary cybersecurity measures according to their classification.
- **Support and assistance:** Provide support and assistance to entities in implementing compliance requirements, including training and technical resources.

4.5. Monitoring and re-evaluation

4.5.1. Continuous monitoring

- **On-going surveillance:** Implementation of a continuous monitoring system to assess the compliance of entities with the requirements of the NIS 2 Directive and to detect possible changes that could affect classification.
- **Regular feedback:** Collect regular feedback from entities and stakeholders to assess the effectiveness of implemented measures and identify areas for improvement.

4.5.2. Periodic reassessment

- **Annual reviews:** Carrying out reviews annually or at set intervals to reassess the classification of entities, taking into account changes in economic size, production capacity and other relevant variables.
- **Updating the classification:** Adjust the classification according to new data and assessments, ensuring that all entities remain compliant and up to date with the requirements of the NIS 2 Directive.

This detailed final classification step ensures that all food business entities are correctly assessed and classified and that cybersecurity measures are implemented in a manner commensurate with the importance and impact of each entity. This process contributes to the overall security and resilience of the food sector, protecting it against cyber threats and ensuring continuity of supply and food safety.

SECTION 3. RECORDS OF ENTITIES

In this section, emphasis is placed on the importance of documenting the processes of identification and classification of entities to which the NIS 2 Directive is applicable in the food sector. Adequate record-keeping is essential to ensure transparency and accountability in cyber risk compliance and management processes.

PRINCIPLES OF RECORD OF ENTITIES

#1. Definition of identification criteria

Specific approaches

- **Membership in the food sector:** Registration of the CAEN code and verification of the main activities of the entity, as defined by the food sector. For example, sector-specific NACE codes can be used to identify the field of activity (production, distribution, retail).
- **Fulfilment of the special criteria:** Verification of compliance with additional requirements, such as national food safety regulations or other specific rules.
- **Size of economic entity:** The collection of data on turnover, number of employees and production volume, which will help to determine whether the entity is considered small, medium or large.

#2. Classification of entities

Economic entities

- **Essential entities:** Criteria such as significant impact on the food market, distribution capacity or strategic importance in national and regional supply.
- **Important entities:** Entities that do not meet all the criteria to be essential but still have a relevant role in regional or sectoral sourcing.
- **Non-critical entities:** These are entities that do not fall into the categories of high importance but contribute to the local food economy.

National Competent Authority

- **Register of essential and important entities:** is established and maintained at the level of the national competent authority (in Romania and Bulgaria respectively).

#3. Creation of a centralised database

Steps to create centralized databases

- In order to identify essential and important entities in the food sector (as well as non-critical entities reporting on **a voluntary basis), once the identification process and the classification process have been completed, qualified and classified economic entities are required to submit a notification to the relevant national competent authority (in Romania and Bulgaria respectively).**
  - ✓ **The notification shall contain** at least the following information: the name, address and up-to-date contact details, including the entity's email addresses, IP series and telephone numbers, the name and contact details of the liaison person and, where applicable, the sector, as well as, where

applicable, a list of Member States where it provides services falling within the scope of the NIS 2 Directive.

- ✓ At the same time, for the final classification of the economic entity classified as an entity to which the NIS 2 Directive applies, **the classified economic entity will submit an assessment of the level of cybersecurity maturity.**

➲ The electronic platform where all data collected for each food business entity is stored, including identification, classification and regular updates, shall allow easy entry, access and modification of the data by the record management team.

- ✓ In the case of this project, once the **"Platform for national and cross-border cooperation NIS – Romania and Bulgaria" [CORB] has been implemented and operationalised, the data and information will be completed/introduced by the economic entity directly into the platform** and the assessment of the cybersecurity maturity level will be carried out at platform level.

➲ After taking into account the critical entity, **the entity shall be required to notify without delay any changes to the details submitted** pursuant to the second subparagraph of this Section, and in any event within two weeks from the date of the change.

#4. Documentation of the identification and classification process

Documentation

➲ **Highlighting the criteria used:** Document each step of the identification and classification process, with clear references to the specific criteria used (NACE code, economic dimension, role in the supply chain).

➲ **Sources of information:** Record primary sources of information (financial reports, regulators, official registers) used for the assessment of each entity.

#5. Reporting and transparency

Reporting

➲ **Annual reporting:** Create assessment and update reports that are available to competent authorities, ensuring the transparency of the process.

➲ **Controlled access:** Limiting access to the database to ensure the protection of sensitive information, in line with cybersecurity requirements.

#6. Regular updating of the record

Regular updates

➲ **Periodic evaluations:** Establish a timeline for the annual assessment of establishments, taking into account economic and risk changes in the food sector.

➲ **Continuous monitoring:** Implement an automated monitoring system to alert if an entity changes its status or economic data.

#7. Protecting data privacy and security

Confidentiality

- **Cybersecurity:** Ensuring the confidentiality and integrity of the data stored in the filing system through encryption and other security measures. This is essential to protect sensitive information about food business entities.
- **GDPR compliance:** Personal and commercial data must be handled in accordance with data protection legislation, such as the General Data Protection Regulation (GDPR).

At the level of the national competent authority

- An **automated monitoring system** will also be put in place to alert if an entity changes its status or economic data.
- Depending on the assessment and decision needs of the national competent authority, **further data on the identification and classification processes may be required.**

This filing system allows clear and detailed management of entities, respecting the criteria of the identification and classification methodology and facilitating compliance with the NIS 2 Directive in the food sector.

CONCLUSION

This *Guide* provides a structured framework for the identification, classification, and documentation of economic entities in the food sector in accordance with the NIS 2 Directive requirements. By applying this framework, sector operators can not only accurately identify entities needing enhanced cybersecurity measures but also maintain a clear and up-to-date registry, thus better equipping themselves to respond effectively to cyber risks.

The identification process ensures that all relevant entities are covered, while classification enables the prioritization of security measures based on criticality and vulnerability specific to the food sector. Maintaining detailed and current records facilitates continuous monitoring and provides authorities with a quick assessment tool in case of an incident.

To strengthen this management system, we recommend:

1. **Regular updates to classification criteria** to reflect changes in the cyber threat landscape.
2. **Enhanced collaboration** between the food sector and national security authorities, ensuring transparency and coordination in the protection of essential infrastructure.
3. **Establishing regular audit procedures** to verify the compliance of identified entities and to assess the effectiveness of security measures.

By adopting these best practices, economic entities within the food sector will not only align their operations with the requirements of the NIS 2 Directive but will also actively contribute to strengthening cybersecurity resilience at both national and European levels.

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.