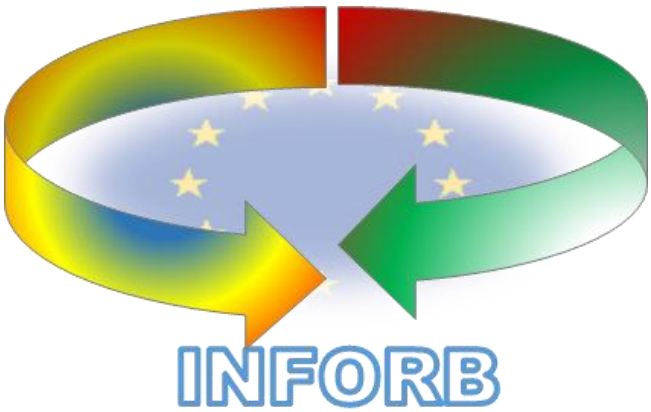

GOOD PRACTICE GUIDE REGARDING THE IMPLEMENTATION OF THE NIS 2 DIRECTIVE AT THE LEVEL OF THE FOOD SECTOR

DELIVERABLE D2.2

Version 2.0

15.07.2025

SUMMARY

This "Guide to good practices on the implementation of the NIS 2 Directive in the food sector" (deliverable D2.2, version 2.0) offers a series of recommendations and solutions for ensuring and strengthening the security of networks and information systems, with a focus on the essential stages of the implementation process, in accordance with the Government Emergency Ordinance no. 155/2024 on certain measures implementing Directive (EU) 2022/2555 (NIS Directive 2).

GEO no. 155/2024 establishes concrete cybersecurity requirements for critical infrastructures, including the food sector, given the increased risks generated by digitalization and interconnectivity. Entities in this sector must adopt appropriate and proportionate measures to protect networks and information systems against cyber threats, in line with the new legal obligations.

The guide includes detailed steps on the "identification, classification and record-keeping" of essential and important entities in the food sector, in accordance with the reporting and notification requirements provided by GEO no. 155/2024. These steps are essential for the initial preparation of the compliance process and for a correct understanding of the vulnerabilities specific to the food sector, facilitating the development and implementation of a coherent plan of cybersecurity measures.

The guide also provides good practices for stakeholder identification, risk management, incident prevention, notification of security incidents and protection of the food supply chain, in accordance with the provisions of GEO no. 155/2024 and the requirements imposed by the competent authorities (DNSC, ANSVSA).

By disseminating this guide, we aim to support all entities in the food sector in adopting the necessary measures for compliance with GEO no. 155/2024 and the NIS 2 Directive, thus contributing to reducing digital vulnerabilities and strengthening cyber resilience in this strategic 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.

Information on document control

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 food production, processing and distribution sector in Romania and Bulgaria.
Project acronym:	INFORB
Author(s) document:	Gabriel HÎMPĂ
Deliverable identifier:	D2.2
Due date of delivery:	31.07.2025
Delivery date:	15.07.2025
Project Manager (MP):	Constantin Călin
Document version:	V2.0
Sensibility:	PU-Public
Date:	15.07.2025

Document appraisers and appraisers

Name	Role	Action	Date
Gabriel HÎMPĂ	Leader of Working Group 2	Draft Document Created	15.09.2024
Gabriel HÎMPĂ	Leader of Working Group 2	Original Version (DNSC)	08.10.2024
Mihai Guranda	Project Assistant Manager	Quality assurance version	31.10.2024
Gabriel HÎMPĂ	Leader of Working Group 2	Updated version	15.07.2025
Constantin CĂLIN	Project Manager	Final document assumed and delivered	15.07.2025

Document history

Revision	Date	Created by	Brief description of the changes
V0	15.09.2024	Leader of Working Group 2	Document created
V0.1	30.10.2024	Leader of Working Group 2	Rectification of the updated document with information
V1.0	31.10.2024	Leader of Working Group 2	Updating the document
V2.0	15.07.2025	Leader of Working Group 2	Updating the document

Contained

INTRODUCTION

The "*Good Practice Guide on the Implementation of the NIS 2 Directive in the Food Sector",* hereinafter referred to as *the Guide*, is developed within the project "Implementation of the NIS Directive in the Food Production, Processing and Distribution Sector in Romania and Bulgaria" (INFORB), co-funded by the European Commission, with the aim of supporting companies in **the food** production, processing and distribution sector in the application of cybersecurity requirements, in accordance with **Directive (EU) 2022/2555 (NIS 2), Government Emergency Ordinance no. 155/2024**, the normative act transposing NIS 2 into Romanian legislation and Law **no. 124 of 7 July 2025** for the approval of Government Emergency Ordinance no. 155/2024 on the establishment of a framework for the cybersecurity of network and information systems in national civil cyberspace.

As of October 17, 2024, the food sector is officially included in the list of sectors of **essential and important importance** according to Annex 2 of GEO 155/2024. Thus, the economic entities operating in this sector – regardless of the form of organization – may fall under the identification**, classification, notification and reporting** obligations provided by the national legislation and orders of the National Directorate of Cyber Security (DNSC).

This guide also reflects the changes brought by **the Order on the methodology for identifying and classifying entities, a** document developed by DNSC for standardizing the compliance process. Essential elements include:

- registration through **the NIS2@RO platform**,
- annual cybersecurity maturity self-assessment,
- designation of the person responsible for cybersecurity,
- reporting incidents within the stipulated deadlines (24h, 72h, 1 month),
- periodic audits according to the level of risk.

The food sector, while traditionally perceived as low-level technology, has become **highly digitized and interconnected**, exposing itself to increasingly sophisticated cyber risks. In this context, the guide aims to support:

- **identification of relevant entities**,
- **classifying them** into essential, important or non-critical entities,
- **compliant registration and reporting** in national platforms,
- and **the adoption of cybersecurity measures commensurate** with the risks.

The goal is to contribute to the **digital resilience of the food chain** in Romania and to align security practices at European level. The guide provides a uniform methodological framework and can be adapted according to subsequent legislative changes or updates issued by the DNSC.

Purpose

The Good Practice Guide is designed to provide **clear, operational guidelines and in line with the requirements of GEO no. 155/2024**, the normative act transposing the NIS 2 Directive in Romania, **Law no. 124 of 7 July 2025** for the approval of Government Emergency Ordinance no. 155/2024 on the establishment

of a framework for the cybersecurity of network and information systems in the national civil cyberspace, as well as with the **DNSC Methodology** on the identification and classification of entities.

The main purpose is to support entities in the **food** sector – production, processing, distribution, storage, retail, food services – in:

- **understanding the legal obligations** arising from the applicability of the NIS 2 Directive.
- **correctly identifying** the entities to which the regulations apply.
- **their classification** as essential or important entities.
- and **the implementation of the technical and organizational cybersecurity measures** provided for by the updated legislation.

The guide also has a **pedagogical and preventive role**, providing models of good practices and standardized operational steps to support entities in aligning with national and European requirements on **cyber resilience**.

Objectives

Ensuring compliance with the NIS 2 Directive

- A first objective of the implementation of the NIS2 Directive is **to ensure compliance with it** in the food sector by involving:
  (1) promoting and ensuring robust and effective cybersecurity in the critical infrastructures of entities in this sector.
  (2) providing a clear framework for understanding the requirements.
- The transposition of the requirements of the NIS 2 Directive into the Romanian legal framework through GEO 155/2024 imposes compliance obligations on entities in the food sector (identification, registration, reporting, technical measures).
- The guide provides a methodological framework that supports entities to understand **whether and how their obligations are applicable**, register in the DNSC platform (NIS2@RO) and avoid sanctions.

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 can include data processing systems, distribution networks, production management systems, etc.
- This is essential to ensure **the continuity of food supply** and the protection of public health.

Implementation of cybersecurity measures

- According to Article 13 of GEO 155/2024, entities must implement measures such as: **risk management, encryption, access control, incident response, backup, testing,** auditing, etc.
- The guide provides examples and recommendations on the implementation of these measures, adapted to the specifics of the food sector.

Cybersecurity risk assessment and management

- Entities are required to carry out **regular risk assessments** and submit the results through the national platform (ATHENA or NIS2@RO).
- The guide explains the structure of the self-assessment, the minimum criteria and how to document the results.

Business Continuity and Incident Response

- The development of continuity plans and response scenarios in case of cybersecurity incidents is promoted, as required by the legislation (GEO 155/2024, art. 11 letter e).
- The aim is to maintain the essential functioning of food services in situations of digital crisis.

Employee awareness and training

The cybersecurity culture is also an important objective achievable at the level of every economic enterprise through **employee awareness and training (continuous processes),** achieved through awareness sessions and the active involvement of employees in the protection of data, information and information networks and systems.

Monitoring and auditing of network and information systems

In accordance with GEO 155/2024, important and essential entities will be subject to security audits. The process can be achieved by (1) implementing mechanisms for continuous monitoring of networks and information systems for the early detection of possible cybersecurity threats or incidents, and (2) periodic (regular) auditing of networks and information systems to ensure compliance with cybersecurity policies and applicable standards.

SECTION 1. ENTITY IDENTIFICATION

- This section has the role of supporting entities in the food sector in the identification process as regulated entities under GEO no. 155/2024, which transposes Directive (EU) 2022/2555 (NIS 2) and Law no. 124 of 7 July 2025 for the approval of Government Emergency Ordinance no. 155/2024 on the establishment of a framework for the cybersecurity of networks and information systems in the national civil cyberspace
- According to art. 2 and Annex 2 of GEO 155/2024, the "food production, processing and distribution" sector is regulated as a sector of essential importance, and the entities that compose it can be classified as essential, important or non-critical, depending on their size, impact and role in the supply chain.

STEPS IN IDENTIFYING THE ENTITIES TO WHICH THE NIS 2 DIRECTIVE APPLIES:

This section has the role of supporting entities in the food sector in the identification process as regulated entities under GEO no. 155/2024, which transposes Directive (EU) 2022/2555 (NIS 2) into Romania.

According to art. 2 and Annex 2 of GEO 155/2024, the "food production, processing and distribution" sector is regulated as a sector of essential importance, and the entities that compose it can be classified as essential, important or non-critical, depending on their size, impact and role in the supply chain.

Step 1. Food Membership Verification

The procedure involves assessing the main activities of the economic enterprise to determine whether the activities are the impact of the food sector. Activities may include producing, processing, distributing, selling, or serving food. The first step in the identification process is an essential one to determine whether or not the NIS 2 Directive applies to that entity.

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

1.1. Identification of main activities

1.1.1. Definition of food activities

- **Agricultural and food production (NACE 01, 10, 11):** Activities involved in the cultivation, harvesting and growing of food raw materials, such as agriculture, fisheries and animal husbandry.
- **Food processing and packaging:** Processing food raw materials into finished products, including activities such as meat processing, dairy manufacturing, vegetable and fruit preservation.
- **Storage and distribution (NACE 52, 46):** Transport and storage of food products to points of sale or other intermediaries in the supply chain.
- **Food sales and services: (Retail and HORECA** NACE 56, 55 – only under specific conditions) Retail and wholesale of food products, as well as public catering services, including restaurants, canteens and catering.

1.1.2. Verification of activities

- **Internal Documentation Review:** Review of the entity's internal documents, such as activity reports, financial statements, websites, and marketing materials to identify relevant activities.

- **Interviews and inspections:** Conducting 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. The 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 trade in motor vehicles and motorcycles (relevant groups and classes).
  - ✓ **52** - Storage and auxiliary activities for transport (group 521 – Storage).
  - ✓ **55** - Hotels and other accommodation facilities.
  - ✓ **56** - Restaurants and other food service activities.

1.2.2. Verification of NACE registration

- **Official documents:** Checking the entity's official entries in the trade register and other government databases to confirm the NACE codes under which the entity is registered, respective CAEN rev.2 and rev.3 for Romania / NACE.BG-2008 and NACE.BG-2025 for Bulgaria.

1.3. Licences and authorisations

1.3.1. Verification of compulsory licences

- **Sanitary-veterinary authorizations:** Verification of the existence of the sanitary-veterinary authorizations necessary to carry out food activities.
- **Food safety certifications:** Verification of food safety certifications such as ISO 22000 (Food Safety Management System - international standard for food safety management systems), HACCP (Risk Analysis and Control of Critical Control Points - is a systematic method for identifying, assessing and controlling risks associated with food safety, is focused on preventing food contamination, rather than detecting it in finished products), BRC (British Retail Consortium - is to ensure that suppliers comply with specific requirements for food safety, hygiene, quality control and other relevant standards) or other recognised standards.

1.3.2. Regulatory compliance

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

1.4. Evaluation of the product portfolio

1.4.1. Product/Service Analysis

- **Product categories:** The classification of the goods or services provided by the entity to determine whether they are food or directly related to the food industry.

- **Importance and place of the entity in the food sector:** Assessing the entity's position in the food value chain to understand its role and impact in the sector.

1.4.2. Marketing information

- **Promotional materials:** Review of promotional materials 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 material suppliers, distributors and main customers.
- **Contracts and agreements:** Review of contracts and agreements to confirm the nature of activities and membership in the food sector.

1.5.2. Feedback from partners

- **References:** Soliciting 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 summarizing the evaluation process, the criteria used and the conclusions regarding the entity's membership in the food sector.
- **Justifications:** Provide justifications and evidence 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 approve it 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 solid basis for subsequent assessments and classifications.

Stage 2. Fulfilment of special criteria

The stage involves the assessment of the entities identified in the previous phase to verify that 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.

2.1. Safety and Security Impact Assessment

2.1.1. Impact on food security

- **Risk analysis:** Assessing the risks associated with the entity's activities that could affect food security, including cyber risks that could disrupt the supply chain or food production;

- **Incident scenarios:** Developing and assessing possible cyber incident scenarios and their impact on food safety.

2.1.2. Impact on public health

- **Hazard assessment:** Analysis of potential public health hazards caused by supply chain disruptions or compromised food integrity due to cyber-attacks;

2.2. Assessment of dependence on critical infrastructures

2.2.1. Related critical infrastructures

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

2.2.2. Vulnerability assessment

- **Identification of vulnerable points:** Analysis of the vulnerable points of the critical infrastructures on which the entity depends and the potential chain effects of a cyber incident.
- **Safeguards:** Verification of the safeguards in place to secure these critical interdependencies and prevent the propagating 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.

2.3.2. Social impact

- **Role in the community:** Assessing 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 of the cybersecurity policies implemented by the entity to ensure adequate protection of networks and information systems.
- **Response Procedures:** Evaluating incident response procedures and business continuity plans to manage and minimize the effects of cyber incidents.

2.5. Assessment of incident response capacity

2.5.1. Equipment and technologies

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

2.5.2. Human resources and training

- **Specialized personnel:** Assessment of the availability and competencies of specialized cybersecurity personnel.
- **Training programmes:** Verification of the existence of continuous training programmes for staff in order to maintain and improve incident response capacities.

2.6. Evaluation report and documentation

2.6.1. Centralisation of results

- **Detailed report:** Preparation of a detailed report summarising the results of the evaluation 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

- **Document Records:** Maintaining a complete and well-organized record of all documents and information used in the evaluation process.
- **Periodic Review:** Establishing a process for periodic review of documentation to reflect necessary changes and updates.

These intermediate steps ensure a complete and detailed assessment of entities in the food sector, facilitating the correct identification of those that need to comply with the NIS 2 Directive. This establishes an effective framework for protecting critical infrastructure and ensuring food security at national and European level.

Stage 3. Size of the economic entity

The stage involves assessing the economic dimension of food businesses in the food sector to determine their eligibility in accordance with GEO 155/2024 and the NIS 2 Directive. The economic dimension is an essential criterion in determining the impact and relevance of entities in the food sector, helping to ensure compliance with cybersecurity requirements.

The size represented by thresholds that are calculated on the basis of figures for the entire legal entity (including all its activities, even outside the EU), strengthened proportionally to the figures of the partner or related companies.

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

Useful links for establishing 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
- 'SME Definition User Guide' (European Commission): https://op.europa.eu/en/publication-detail/-/publication/756d9260-ee54-11ea-991b-01aa75ed71a1
- SME Self-Assessment Tool (European Commission): https://ec.europa.eu/growth/tools-databases/SME-Wizard .

3.1. Assessment of the economic dimension

3.1.1. Size criteria

- **Number of employees:** Assessment of the average number of employees over the course of a financial year. This is a primary indicator of the economic size of the entity.
- **Turnover:** The analysis of annual turnover, which reflects the total revenues generated by the entity in a financial year.
- **Total assets:** A valuation of the total value of the assets held by the entity, including land, buildings, equipment, and other property.

3.1.2. Size thresholds

- **>250 employees and/or >50 mil. EUR turnover/43 mil. EUR assets** = essential entity
- **Between 50–250 employees or between 10–50 mil. EUR CA** = important entity
- Below these thresholds: possibly **non-submissive**, with exceptions (systemic role, special regulation)
- **Micro-enterprises:** Entities with fewer than 10 employees and an annual turnover or total assets of less than €2 million.
- **Small businesses:** Entities with fewer than 50 employees and an annual turnover or total assets of less than €10 million.
- **Medium-sized enterprises:** Entities with fewer than 250 employees and an annual turnover of less than €50 million or total assets of less than €43 million.
- **Large enterprises:** Entities that exceed the limits set for small and medium-sized enterprises.

3.2. Evaluation methodology

3.2.1. Collection of financial data

- **Data sources:** Use of annual financial reports, balance sheets and other relevant financial documents to collect the data necessary to assess the economic dimension.

- **Historical data:** Collecting and analysing financial data over several years to identify trends and ensure the accuracy of the evaluation.

3.2.2. Data validation

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

3.3. Data analysis and interpretation[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 the total revenue generated from the sale of products and services.
- **Total assets:** Determination of the total value of assets by summing the book value of all assets held.

3.3.2. Comparison with size thresholds

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

3.4. Assessment of structural complexity

3.4.1. Analysis of the organizational structure

- **Management structure:** Assessment of the management structure and hierarchical levels within the entity to determine organizational complexity.
- **Divisions and departments:** Analysing the number and functions of divisions and departments in the entity to assess operational complexity.

3.4.2. Assessment of operational complexity

- **Supply chain:** Analysis of the complexity of the supply chain and the number of partners and suppliers involved.
- **Technological processes:** Assessing 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 dimension of the entity.

[1] In order to determine the data to be examined and evaluated against the thresholds, an undertaking must first determine whether it is: (a) a stand-alone undertaking (by far the most common category); (b) a partner undertaking; or (c) an affiliated enterprise.
Depending on the situation, an undertaking should consider: (1) only its own data; (2) part of the data in the case of a partner undertaking; or (3) all data of any undertaking deemed to be affiliated with it.

- **Recommendations**: Providing recommendations for necessary compliance measures based on the economic dimension category to which the entity falls.

3.5.2. Review and approval

- **Internal Review:** Review of the report by the compliance team and entity management to ensure the accuracy and fairness of the assessment.
- **Final approval:** Approval of the report by the entity's management and archiving it for future reference and for use in the subsequent stages of the NIS 2 compliance process.

This detailed stage of assessing the economic dimension 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.

Step 4. Qualification as an entity to which the NIS Directive applies2

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

It is important that these steps are carefully followed and well documented to ensure compliance and effectiveness in managing cyber risks.

4.1. Summary of previous evaluations

4.1.1. Integration of results

- **Food Membership:** Establishing that the entity meets the criteria for food membership based on NACE codes and core activities.
- **Fulfilment of special criteria:** Confirmation that the entity meets special criteria regarding the impact on food security, public health, critical infrastructure, and compliance with cybersecurity standards.
- **Economic dimension:** Verification that the entity falls within the relevant economic dimension thresholds for the NIS2 Directive (micro, small, medium or large enterprises).

4.1.2. Integrated assessment

- **Integrated analysis:** Combining the results of previous assessments into an integrated report concluding the status of the entity in each of the previous steps.
- **General compliance:** Assessment of the entity's overall compliance based on multiple criteria to determine whether it must comply with the NIS2 Directive.

4.2. Assessment of the potential impact

4.2.1. Impact on national security

- **Role in national security:** Assessing the entity's role in maintaining food security and other critical infrastructure at national level.

- **Risk potential:** Determining 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 networks and information systems used by the entity.
- **Critical vulnerabilities:** Identification of critical vulnerabilities and potentially exploitable access points in the entity's networks and information systems.

4.3. Compliance with legal and regulatory requirements

4.3.1. Cybersecurity requirements

- **Security standards:** Verifying the entity's compliance with international and national cybersecurity standards such as ISO/IEC 27001.
- **Policies and procedures:** Assessing the existence and effectiveness of the 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 NIS2 Directive, including the notification of cybersecurity incidents.
- **Transparency and accountability:** Assessing the level of transparency and accountability of the entity in reporting and managing security incidents.

4.4. Final determination of qualification

4.4.1. Decision analysis

- **Qualification criteria:** Application of a final set of decision-making criteria to determine whether the entity must comply with the NIS2 Directive.
- **Compliance Score:** Assigning a compliance score based on the results of previous assessments and final decision-making criteria.

4.4.2. Compliance decision

- **Entity classification:** The classification of the entity as subject or not subject to the requirements of the NIS2 Directive.
- **Communication of the decision:** Communication of the final decision to the entity, including a detailed justification of the conclusions and next steps required for compliance.

4.5. Documentation and continuous monitoring

4.5.1. Final qualification report

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

4.5.2. Continuous monitoring

- **Periodic reviews:** Establish a schedule of periodic reviews to update assessments and ensure continued compliance with the NIS2 Directive.
- **Updating information:** Keeping information up to date about the economic size, organizational structure, and compliance of the entity.

This final classification step ensures that all relevant entities in the food sector are correctly identified and in accordance with the requirements of the NIS2 Directive. The detailed assessment and qualification process contributes to the security and resilience of critical infrastructures, thereby protecting food security and public health.

Stage 5. Notification and Registration

5.1. Notification obligation

- Within 30 days of identification/self-assessment, the entity must register in the NIS2@RO platform, managed by DNSC.

5.1. Content of the notification (minimum)

- Name, headquarters, NACE, contact details.
- Field of activity and sector.
- Name of the person responsible for cybersecurity
- Economic Dimension Statement
- List of EU Member States where they work (if applicable)

- **The DNSC has the right to reassess the status of an entity at any time** and request additional information or audits.
- Entities must keep identification**, classification and notification documentation** for a minimum of 5 years.
- An **annual review** of the bylaws is recommended as part of the ongoing compliance process.

SECTION 2. CLASSIFICATION OF ENTITIES

STEPS IN THE CLASSIFICATION OF ENTITIES ACCORDING TO IMPORTANCE

The classification of economic entities in the food sector into **essential**, **important** or **non-critical** is carried out according to Article 4 of GEO no. 155/2024 and the methodology provided for in **the DNSC Order on the identification and classification of regulated entities**.

The purpose of this stage is to determine the **critical level and exposure to cyber risks**, in order to differentiate the application of the security and reporting obligations provided by the legislation.

Stage 1. Assessment of the quality of essential entity (GEO 155/2024, art. 4 para. (2))

Assessment criteria and process for determining essential entities:

(1) it has over **250 employees**.
(2) it has an annual turnover of **over 50 million euros** or total assets of over **43 million euros**.
(3) **carries out activities in the essential sector** listed in Annex 2 of GEO 155/2024, including **the food sector**.

1.1. Identification of evaluation criteria

1.1.1. Importance

- **Role in the supply chain:** Assessing the entity's position in the food supply chain and its importance in the continuous supply of essential food products.
- **Critical interdependencies:** Identifying critical interdependencies with other entities and infrastructures that could affect the continued functioning of the food sector.
- **Sole Supplier or Entity** with National/Strategic Coverage

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 public health impact 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 entity's production and distribution capacity 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. Evaluation methodology

1.2.1. Data collection and analysis

- **Data sources:** Using internal reports, market data, and information from relevant authorities to collect data on the systemic importance and potential impact of the entity.
- **Interviews and consultations:** Conducting interviews and consultations with food industry experts, regulators and other stakeholders to gain additional insights.

1.2.2. Risk assessment

- **Incident scenario analysis:** Risk assessment by analysing hypothetical cyber incident scenarios and their impact on the entity's operation and food security.
- **Mitigation measures:** Identifying the entity's existing measures and response capabilities to manage and mitigate cyber risks.

1.3. Determination of essential entity status

1.3.1. Setting assessment thresholds

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

1.3.2. Final classification

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

1.4. Communication and monitoring

1.4.1. Informing entities

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

1.4.2. Continuous monitoring

- **Periodic reviews:** Establish a schedule of periodic reviews to reassess the classification of entities and ensure continued compliance with GEO no. 155/2024 and the NIS2 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 stage of assessment of the quality of essential entity ensures the correct identification of the entities that play an essential role in the food sector and that must comply with the requirements of GEO no. 155/2024 and the NIS2 Directive to maintain cybersecurity and resilience of critical infrastructures.

Stage 2. Assessment of the quality of important entity Main criteria (GEO 155/2024, art. 4 para. (3))

The stage focuses on identifying and assessing entities that, although not classified as essential, have a significant role in the food sector and must comply with the requirements of GEO no. 155/2024 and 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 entity is classified as **important** if:

- it has between **50 and 250 employees** and a turnover between **10 and 50 million euros** or assets between **10 and 43 million euros**.
- operates in a sector covered by GEO 155/2024 (including the food sector – Annex 2).

Even entities below the above thresholds can be classified as important if:

- are designated by decision of the DNSC,
- provides critical services for an essential entity,
- were previously classified as important (until re-evaluation).

2.1. Identification of evaluation criteria

2.1.1. Importance in the supply chain

➲ **Contribution to supply:** Assessment of the entity's contribution to 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 the event of incidents.

2.1.2. Impact on consumers

➲ **Geographical spread:** Assessment of 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 capacity

➲ **Operational resilience:** Assessing the entity's ability to respond and recover quickly in the event of cyber incidents or other disruptions.

➲ **Continuity plans:** Verification of the existence and effectiveness of business continuity plans and risk mitigation measures.

2.2. Evaluation methodology

2.2.1. Data collection and analysis

➲ **Data sources:** Use of data from activity reports, information from relevant authorities and market studies to collect the information necessary for the assessment.

- **Stakeholder consultations:** Holding consultations with food industry representatives, regulators and experts to gain a comprehensive perspective on the importance of the entity.

2.2.2. Risk and vulnerability assessment

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

2.3. Determination of significant entity status

2.3.1. Setting assessment thresholds:

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

2.3.2. Final classification

- **Score analysis:** The calculation and analysis of the scores obtained based on the criteria established to determine whether the entity qualifies as a significant entity.
- **Process documentation:** Preparation 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. Informing entities

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

2.4.2. Continuous monitoring

- **Periodic reviews:** Establishing a calendar of periodic reviews to reassess the classification of entities and ensure continued compliance with GEO no. 155/2024 and the NIS2 Directive.
- **Updating information:** Keeping information up to date about the economic dimension, organizational structure, and responsiveness of the entity.

This detailed significant entity quality assessment step ensures that all relevant entities in the food sector are correctly identified and appropriately classified to comply with the requirements of the NIS2 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 phase focuses on identifying entities that, although part of the food sector, are not considered essential or important according to the criteria of the NIS Directive2.

Non-critical entities have a lower impact on food security and the supply chain, having a lower exposure and risk in the event of a cyber incident.

Entities are considered **non-critical** if:

- do not reach the minimum economic thresholds (less than 50 employees and less than 10 mil.). EUR CA).
- are not involved in systemic or critical infrastructure functions.
- does not provide services to classified entities.

Important mentions:

- Classification as non-critical **does not exclude cybersecurity obligations**, if the entity decides to voluntarily implement a protection system.

Non-critical entities may be reassessed by the DNSC in the event of a change in size, structure or contractual relationships.

3.1. Identification of evaluation criteria

3.1.1. Size and economic capacity

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

3.1.2. Reduced 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 small number of consumers or entities dependent on the products and services provided.

3.1.3. Resilience of systems

- **Support systems:** entities that have a surplus of information in their operating and support systems, reducing the risk of impact in the event of an incident.
- **Resilience:** assessment of the entity's ability to recover quickly in the event of disruptions, with minimal impact on consumers and the supply chain.

3.2. Evaluation methodology

3.2.1. Data collection and analysis

- **Data sources:** the use of data from financial reports, risk assessments and information from regulators to collect information about the size and capacity of the entity.
- **Stakeholder consultations:** conducting consultations with entities, experts and authorities to validate the information collected and gain additional insights.

3.2.2. Risk and vulnerability assessment

- **Specific risk analysis:** assessment of the specific risks associated with the entity's operations, considering the limited impact on food security and the supply chain.
- **Incident impact:** analysis of the potential impact of incidents on the entity's operations, focusing on local risks and minimal impact on consumers.

3.3. Determination of non-critical entity status

3.3.1. Setting assessment thresholds

- **Qualitative and quantitative criteria:** Definition of qualitative criteria (e.g. local importance, system capacities – implementation of backup measures or duplication of components or functions of a system to ensure continuity of its operation in the event of failures or errors) and quantitative criteria (e.g. production capacity, turnover) to assess low importance.
- **Performance indicators:** Assigning performance indicators for each criterion to facilitate the assessment and comparison of entities.

3.3.2. Final classification

- **Score analysis:** The calculation and analysis of the scores obtained based on the criteria established to determine whether the entity qualifies as a non-critical entity.
- **Process documentation:** Preparation 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. Informing entities

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

3.4.2. Continuous monitoring

- **Periodic reviews:** Establishing a calendar of periodic reviews to reassess the classification of entities and ensure continued compliance with GEO no. 155/2024 and the NIS2 Directive.
- **Updating information:** Keeping information up to date about the economic dimension, organizational structure, and responsiveness of the entity.

Through this detailed non-critical entity quality assessment step, it is ensured that all entities in the food sector are correctly classified, thus contributing to effective risk management and cybersecurity protection, even for

low-impact entities. This detailed process helps to clarify responsibilities and allocate security resources in proportion to the importance of entities in the food sector.

Step 4. Final classification of entities

The stage represents the culmination of the process of evaluation and classification of entities in the food sector according to GEO no. 155/2024 and the NIS2 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 proportionate to their role and impact.

According to the DNSC order:

- **the entity must submit the** self NIS2@RO-assessment report and notification **through the platform within 30 days** of the completion of the identification process.
- the classification is validated by the DNSC, which may request further clarification.

Confirmation and inclusion in the register

- DNSC introduces the entity in **the National Register of Essential and Important Entities**, with restricted access according to the provisions of the GDPR.
- The entity shall receive a formal notification of the **assigned category** and the specific compliance deadlines.

4.1. Synthesis and analysis of evaluation data

4.1.1. Centralisation of intermediate outputs

➲ **Outcomes of the previous stages:** Collection and review of the results of the 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:** Assessment of the cumulative impact of entities on the food sector, considering interdependencies and redundancies in the supply chain.

➲ **Identification of key entities:** Identification of entities that, although they may be individually classified as non-critical or important, together play a critical role in ensuring food security.

4.2. Validation and verification of the process

4.2.1. Consistency check

➲ **Internal review:** Conducting an internal review to verify the consistency and correctness of the evaluation and ranking process, ensuring that all criteria have been applied uniformly.

➲ **External audit:** Where necessary, request an external audit to validate the process and results obtained, providing an objective and independent perspective.

4.2.2. Adjustment of assessments

➲ **Feedback and revisions:** Integrating feedback received from stakeholders, experts and authorities, and adjusting assessments where necessary to reflect changes or comments received.

- **Data Update:** Updating valuation data based on recent changes in economic size, production capacity and other relevant variables.

4.3. Determination of the final classification

4.3.1. Setting the final thresholds

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

4.3.2. Preparation of the final report

- **Process documentation:** Preparation of a detailed report documenting the entire evaluation and classification process, including the methodology, the criteria used, the results obtained and the final decisions.
- **Justification of decisions:** Providing a clear and detailed justification for the classification of each entity, based on the data and analysis carried out.

4.4. Communication and implementation

4.4.1. Communication of classification

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

4.4.2. Implementation of compliance requirements

- **Compliance Guidelines:** Providing guidance and recommendations for entities on the necessary cybersecurity measures based on their classification.
- **Support and assistance:** Providing 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

- **Permanent supervision:** Implementation of a continuous monitoring system to assess the compliance of entities with the requirements of GEO no. 155/2024 and the NIS2 Directive and to detect possible changes that could affect the classification.
- **Regular feedback:** Collecting regular feedback from entities and stakeholders to assess the effectiveness of the measures implemented and identify areas for improvement.

4.5.2. Periodic review

- **Annual reviews:** Conducting annual reviews or at set intervals to reassess the classification of entities, considering changes in economic size, production capacity and other relevant variables.

- **Classification update:** Adjusting the classification according to new data and assessments, ensuring that all entities remain compliant and up to date with the requirements of GEO no. 155/2024 and the NIS2 Directive.

Practical recommendations

- Use the self-assessment form provided by the DNSC (it will be published with the final order);
- Ask for legal support or technical advice for the correct classification.
- Maintain supporting documentation and internal decisions related to classification.
- Review the organization's situation (size, activities, customers, etc.) annually to detect any changes that require reclassification.

This detailed final classification step ensures that all entities in the food sector are correctly assessed and classified and that cybersecurity measures are implemented in proportion to 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. ENTITY RECORDS

This section details the steps and obligations related to **the registration, updating and management of the records of regulated entities** in the food sector in the context of the NIS 2 Directive. According to GEO no. 155/2024, the record is managed by **the DNSC**, and the entities classified as essential or important have **the legal obligation** to notify and update.
Proper accounting is essential to ensure transparency and accountability in compliance and cyber risk management processes.

PRINCIPLES OF ENTITY RECORDS

Centralization and record keeping

- It is carried out through the NIS2@RO electronic platform, which is under the administration of the DNSC.
- The platform allows for the digital registration, modification, evaluation and auditing of entities.

Notification obligation (art. 8 GEO 155/2024)

- Entities must submit the classification notification within **30 days** of the self-assessment or DNSC notification.
- The notification is considered transmitted at the time of uploading and electronic signature through the platform.

#1. Definition of identification criteria

Specific approaches

- ⌘ **Membership in the food sector:** Registration of the NACE code and verification of the main activities of the entity, according to the definition of the food sector. For example, sector-specific NACE codes can be used to identify the field of activity (production, distribution, retail).
- ⌘ **Fulfilment of special criteria:** Checking compliance with additional requirements, such as national food safety regulations or other specific rules.
- ⌘ **Size of the economic entity: Collection of** data on turnover, number of employees and production volume, which will help 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 the 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:** it is established and kept at the level of the national competent authority (in Romania and Bulgaria respectively).

#3. Create a centralised database

Steps to create centralized databases

- To consider the essential and important entities in the food sector (but also the non-critical entities that report voluntarily), after the completion of the identification process and the classification process, **the qualified and classified economic entities have the obligation to submit a notification to the corresponding national competent authority (in Romania and Bulgaria respectively).**
  - ✓ **The notification shall include** at least the following information: name, address and updated contact details, including email addresses, IP series and telephone numbers of the entity, name and contact details of the liaison person and, where applicable, the sector and, where applicable, a list of Member States where it provides services falling within the scope of the NIS 2 Directive.
  - ✓ At the same time, with a view to the final classification of the classified economic entity as an entity to which the NIS 2 Directive applies, **the classified economic entity will submit an assessment of the cybersecurity maturity level**.
- The electronic platform where all the data collected for each entity in the food sector is stored, including identification, classification and periodic updates, allows the data to be easily entered, accessed and modified by the records management team.
  - ✓ In the case of this project, after the implementation and operationalization **of the "Platform for National and Cross-Border Cooperation NIS - Romania and Bulgaria" [CORB], the data and information will be completed/entered by the economic entity directly into the platform**, and the assessment of the cybersecurity maturity level will be carried out at the level of the platform.
- Once the essential or important entity have been registered, **the entity shall be required to notify without delay any change in the details submitted** pursuant to the second subparagraph of this section and, in any event, within two weeks of the date of the change.

Content of the notification: According to the DNSC order, the notification sent must contain the following elements:

Required information	Details
Name and legal form	Including CUI and CIF
Contact Date	Address, official email, phone
Relevant NACE codes	In correlation with the actual activity
Entity type	Essential/Important
NIS Responsible Name	If it has already been designated
IT structure	Summary description of networks and systems

Required information	Details
Field of activity	Production, processing, distribution, retail, etc.
Other Member States (if applicable)	Where they provide cross-border services

#4. Documentation of the identification and classification process

Document

- **Highlighting the criteria used:** Documenting 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 of primary sources of information (financial reports, regulators, official registers) used for the valuation of each entity.

#5. Reporting and transparency - Specific obligations (art. 8 para. (2) GEO 155/2024)

Reports

- **Annual reporting:** Creation of evaluation and update reports to be available to the competent authorities, ensuring transparency of the process.
- Any changes to contact details, entity structure, NACEs, or other previously notified information must be submitted to the DNSC within a maximum of 2 weeks from the date of the change.
- The obligation to update is **continuously applicable.**
- **Controlled Access:** Limiting access to the database to ensure the protection of sensitive information, in accordance with cybersecurity requirements.

#6. Regular updating of the record

Regular updates

- **Periodic assessments:** According to the DNSC Order, all entities must carry out **an annual reassessment of cyber classification and maturity**, with the upload of the report to the NIS2@RO platform.
- **The re-evaluation** is correlated with the reporting and self-evaluation cycle.
- **Continuous monitoring:** Implementing an automated monitoring system to alert if an entity changes its status or economic data.

#7. Security maturity assessment

- Entities must annually complete a **standardized maturity self-assessment tool**, provided by the DNSC in the platform.
- The purpose is to measure the progress on the implementation of the measures provided for in art. 13 of GEO 155/2024 (technical and organizational measures).
- The answers will influence the frequency of the audit and the prioritization of DNSC controls

#8. National Register of Entities

- DNSC administers **the National Register of Essential and Important Entities**, in secure electronic format.
- The information in the register can be consulted by the competent authorities, only for regulated purposes (control, audit, incidents, public policies).
- Public access is limited, except in situations expressly provided for by law.

#9. Protecting data privacy and security

Privacy

- **Cybersecurity:** Ensuring the confidentiality and integrity of data stored in the record system through encryption and other security measures. This is essential for protecting sensitive information about food business entities.
- DNSC administers **the National Register of Essential and Important Entities**, in secure electronic format.
- The information in the register can be consulted by the competent authorities, only for regulated purposes (control, audit, incidents, public policies).
- Public access is limited, except in situations expressly provided for by law.

At the level of the national competent authority

- It will also implement **an automatic monitoring system** to alert if an entity changes its status or economic data.
- Depending on the assessment and the decision-making needs of the national competent authority, **additional data on the identification and classification processes** may be requested.

This record system allows for a clear and detailed management of entities, complying with the criteria in the identification and classification methodology and facilitating compliance with GEO no. 155/2024 and the NIS 2 Directive in the food sector by:

- uniform application of the NIS 2 legal framework.
- full traceability of regulated entities.
- effective compliance and risk monitoring.
- rapid intervention in the event of significant incidents.

CONCLUSION

This ***Good Practice Guide*** provides an updated, coherent and practical framework for **the implementation of the NIS 2 Directive** in the food sector in Romania, in accordance with **GEO no. 155/2024** and the **DNSC methodology** in the process of being finalized. It supports actors in the food chain to correctly identify their obligations and to adopt concrete **cybersecurity measures**, according to their critical level.

The guide addresses all the fundamental steps:

- identification of entities in the food sector.
- classifying them as essential, important or non-critical.
- notification and record keeping.
- implementation of technical and organizational measures.
- auditing, risk assessment and incident response.

The application of the methodology in the guide allows:

- alignment with European and national legal requirements.
- reducing operational risks.
- increasing the resilience of the food sector.
- supporting consumer protection and public health.
- effective cooperation with national and European authorities.

To strengthen this management system, we recommend:

1. **Annual review of the entity's statutes in relation to the classification criteria.**
2. **Continuous training** of staff on cybersecurity and incident reporting.
3. **Implementation of the measures provided for in art. 13 of GEO 155/2024** (including access control, incident response, backup, encryption).
4. **Signing up for the NIS2@RO platform** and using it as a work and communication tool.
5. **Regular consultation of legislative updates and DNSC guidelines**.

By adopting these best practices, economic entities in the food sector will not only align their operations with the requirements of GEO no. 155/2024 and the NIS 2 Directive but will actively contribute to strengthening cyber resilience at national and European level.

The digital transformation of the food sector brings **economic benefits**, but also **new vulnerabilities**. In an increasingly complex cyber environment, it is essential that all actors involved – from small manufacturers to regional distributors or large retailers – adopt **a proactive approach, based on prevention, resilience and transparency**.

The adoption of this guide is not just a compliance move, but a strategic investment in **national food security**, **consumer confidence** and **supply chain continuity**.

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.