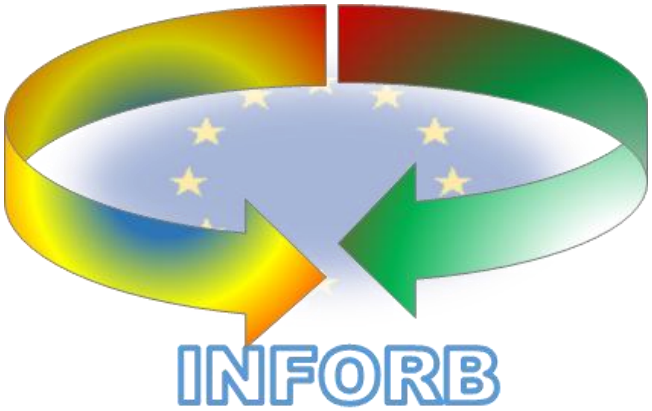

TRAINING SCHEMES FOR THE MANAGEMENT OF ENTITIES AND CYBER SECURITY OFFICERS IN THE FOOD SECTOR

DELIVERABLE D5.2

Version V1.0

EXECUTIVE SUMMARY

This deliverable summarizes the training methodologies, regional implementation strategies, and outcome assessments derived from the INFORB project's focus on strengthening cybersecurity capacity in the food sector of Romania and Bulgaria.

The report highlights the dual-track approach targeting management and cybersecurity personnel, the regional disparities in awareness and readiness, and outlines practical recommendations for sustainable improvement aligned with the NIS2 Directive

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.

Document control information

Settings	Value
Document title:	Training schemes for the management of entities and cyber security officers in 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) of the document:	Bogdan, Radu, Gheorghiță Comăneci, Silviu-Nicolae Dorobanțu, Mihai Rotariu, Gergana Rakova, Eli Kuyamova, Panayotka Panayotova
Deliverable identifier:	D5.2
Delivery deadline:	31.07.2025
Delivery date:	31.07.2025
Project Manager (PM):	Constantin Călin
Document version:	V1.0
Sensibility:	PU-Public
Date:	30.07.2025

Document evaluation and evaluators

Name	Role	Action	Date
Bogdan Radu	WP5 Coordinator	Draft document created	08.07.2025
Bogdan Radu	WP5 Coordinator	Original version (DNSC)	11.07.2025
Silviu Dorobanțu	Cybersecurity Expert		
Gergana Rakova	Project Coordinator	Update version (MGBEG)	25.07.2025
Eli Kuyamova	Project IT expert		
Panayotka Panayotova	BG Team Project Leader		
Advisory Board of Experts	Evaluation	Agreed version	30.07.2025
Bogdan Radu	WP5 Coordinator	Update version	30.07.2025
Constantin Călin	Project Manager	Final document assumed and delivered	31.07.2025

Document history

Review	Date	Created by	Brief description of the changes
V0	08.07.2025	Cybersecurity Expert	Draft document created. Documentation, analysis of sources. Documentation, analysis of sources.
V0.1	11.07.2025	Cybersecurity Expert &	Updated document with information

		WP5 Coordinator	
V0.1.1	22.07.2025	Cybersecurity Expert & WP5 Coordinator	Updated document
V0.1.2	25.07.2025	Coordinator/Project Leader	Updated by Bulgarian Experts
V0.1.3	28.07.2025	Cybersecurity Expert & WP5 Coordinator	Updated document
V0.1.4	30.07.2025	Advisory Board of Experts	Review
V1.0	30.07.2025	WP5 Coordinator & Cybersecurity Expert	Final document version 1

Contained

SECTION 1. CONTEXT AND OBJECTIVES

The inclusion of the **food sector** in Directive (EU) 2022/2555 (NIS2 Directive) reflects a growing recognition that disruptions to food production, processing, and distribution pose serious risks to public health, economic stability, and national security. The digital transformation of the food supply chain has created a dependency on information systems that are more exposed to cyber threats.

The **INFORB project** responds to this reality by focusing on building cyber resilience in the food sector in both Romania and Bulgaria. Its objective is to support entities in understanding their new obligations under the **NIS2 Directive**, prepare them to identify and report cyber incidents, and foster collaboration across borders.

The project includes:

- Identification and classification of essential and important entities in the food sector.
- Development of cyber awareness and training schemes adapted to specific roles within organizations.
- Design of a cross-border cooperation platform (CORB) to facilitate secure information exchange between Romania and Bulgaria.
- Execution of awareness campaigns to drive adoption of cybersecurity practices and use of the CORB platform.

The **training component** of the project targets two core groups:

1. **Management -** to support strategic decision-making, governance, and legal compliance.
2. **Cybersecurity staff -** to guide those responsible for implementing and overseeing cyber protection measures.

By investing in these training initiatives, INFORB aims to foster a cybersecurity culture that enables entities in the food sector to proactively protect themselves and contribute to the security of the broader European digital ecosystem.

The program's goal is to equip individuals in management roles with the knowledge to make informed decisions about cybersecurity investments and policies, while also preparing cybersecurity officers to implement and manage effective risk management and incident response protocols, in the view of the **NIS2 Directive**. Furthermore, by promoting cross-border collaboration, the program will enable knowledge sharing and mutual assistance, which is essential for addressing the transnational nature of cyber threats.

Cybersecurity awareness is critical for companies because human error remains one of the most significant vulnerabilities in any organization's security posture. Employees who lack proper awareness often fall victim to phishing attacks, inadvertently download malware, or mishandle sensitive data, creating entry points for cybercriminals. In the food sector specifically, where operational technology increasingly intersects with information systems, unaware staff can inadvertently compromise both digital assets and physical production processes. Moreover, a workforce educated in cybersecurity fundamentals serves as the first line of defence, capable of recognizing threats early and responding appropriately. This human centered approach to security is particularly vital as cyber threats become more sophisticated and regulatory frameworks like **NIS2** place greater accountability on organizations to demonstrate comprehensive security measures that extend beyond technical solutions to encompass the entire organizational culture.

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.

SECTION 2. SECTOR-CENTERED TRAINING NEEDS ASSESSMENT

2.1 OVERVIEW OF THE FOOD SECTOR'S DIGITAL FOOTPRINT AND THREAT SURFACE

Under NIS2, the food sector is recognized as both important and critical, yet it faces unique cybersecurity risks that are frequently underestimated. These risks are accentuated by its reliance on interconnected supply chains, legacy systems, automation, and third-party services. Multiple types of threats pose operational, economic, and reputational harm:

Operational Disruption: Cyberattacks such as ransomware can halt production lines or disable logistics systems, leading to food shortages, waste, and revenue loss.

Supply Chain Weaknesses: A large number of food sector entities collaborate with multiple suppliers and logistics partners. A single vulnerability in a partner's system can cascade into a larger incident.

Data Integrity and Safety Risks: Alteration or loss of data relating to food safety, temperature controls, or ingredient traceability can lead to unsafe products reaching the market.

IoT and Automation Exposure: Smart sensors, processing robots, and automated inventory systems are often minimally secured and vulnerable to remote exploitation.

Cyber Espionage or Sabotage: Geopolitical tensions or competitive sabotage may target the food sector to cause public disruption or gain unfair market advantage.

Low Cybersecurity Maturity: Especially in small and medium-sized enterprises, cybersecurity functions are often under-resourced, lacking both technical tools and skilled personnel.

These sector-specific threats require tailored cybersecurity measures, practical awareness at all organizational levels, and strong collaboration between national authorities and the private sector.

The food industry has undergone significant digital transformation, creating an expansive attack surface that spans from farm to table:

- **IoT and Smart Agriculture**: Sensors for monitoring soil conditions, weather, livestock health, and crop growth.
- **Supply Chain Management Systems**: Digital tracking and logistics platforms for product movement.
- **Manufacturing Operations**: Industrial control systems (ICS/SCADA) for food processing and packaging.
- **Cold Chain Management**: Temperature monitoring and control systems for perishables.
- **Enterprise Systems**: ERP, CRM, and other financial or management platforms.
- **E-commerce and Digital Ordering**: Online platforms for B2B and B2C transactions.
- **Food Safety Systems**: Digital traceability and compliance monitoring platforms.

Ransomware incidents targeting this sector increased to 212 in 2024, accounting for 5.8 percent of all such attacks, a rise from 167 incidents in 2023[1]. The food industry is vulnerable to cyberattacks, with no less than 167 ransomware attacks reported in 2023 alone[2], according to a report by The Food and Agriculture Information Sharing and Analysis Center (Food and Ag-ISAC).

[1] https://cybersecurityguide.org/industries/food-and-agriculture/
[2] https://foodinstitute.com/focus/5-cybersecurity-tips-for-2025/

Major Attack Vectors:

1. **Ransomware as a Service (RaaS)**: "RansomHub" emerged as a key player, a ransomware-as-a-service group that gained prominence by offering affiliates lucrative opportunities[3].
2. **Supply Chain Vulnerabilities**: The JBS Foods ransomware attack serves as a crucial case study, forcing shutdown of facilities supplying about one-fifth of America's meat supply[4].
3. **Network Architecture Exploitation**: Attackers exploited network architecture vulnerabilities to move laterally through the organization's systems, raising concerns in the industry after the JBS attack.
4. **IoT and OT Vulnerabilities**: Increasing use of IoT devices leads to an increased attack surface, likely to attract more exploits targeting IoT supply chains[5].

2.2 IDENTIFIED GAPS IN AWARENESS, PRACTICES, AND TECHNICAL CAPABILITIES

Prior to developing the training schemes, the INFORB project team conducted a targeted assessment of cybersecurity status and capacity gaps within the food sector. This assessment drew on survey, expert input, and a review of current practices within entities operating across production, processing, and distribution. In addition, several assessments highlight that a large portion of the food sector, particularly small and medium-sized enterprises (SMEs), lacks a comprehensive understanding of cybersecurity risks and best practices. Many enterprises operate without dedicated cybersecurity personnel, relying instead on generalist IT staff who often lack the specialized expertise required to address modern cyber threats effectively.

It is essential to recognize the direct connection between cybersecurity risks and food safety, especially in environments where critical control points (CCPs) are managed through digital systems such as SCADA and other industrial automation tools. The NIS2 Directive places the food sector under critical infrastructure obligations, which means that disruptions caused by cyber incidents (such as ransomware, system manipulation, or unauthorized access) can have immediate consequences on product integrity and consumer safety. In parallel, food safety frameworks like ISO 22000 and HACCP identify CCPs as essential stages in the production process where failure can lead to unsafe food. Many of these CCPs rely on digital monitoring and control systems, and a successful cyberattack on those systems can cause deviations in temperature, time, pressure, or traceability, parameters that are vital for food safety compliance. For example, if malware disables a temperature sensor in cold storage, or modifies settings in a pasteurization unit, the resulting products may not meet health standards, even if no visible issues are present. Therefore, cybersecurity training for both management and technical staff must include scenarios where cyber incidents affect food safety processes (a mapping of NIS2 Cyber Security to HACCP/ISO22000 Food Safety, including an integrated Safety and Security Strategy). Participants should understand how to identify digital dependencies for each CCP, how to secure these systems, and how to respond when anomalies are detected. Key topics to be addressed in training sessions include network segmentation between IT and OT, secure access control for SCADA, regular backups of control settings, incident reporting procedures, and collaboration between cybersecurity teams and food quality officers. Embedding these elements into training schemes ensures that food sector entities develop both compliance with NIS2 and resilience across the production chain. Ultimately, treating cybersecurity as an integral part of food safety and security (as integrated management system) training builds a culture of cross-functional awareness and helps prevent both economic losses and public health risks.

[3] https://cybersecurityguide.org/industries/food-and-agriculture/
[4] https://www.elisity.com/blog/cybersecurity-for-food-manufacturing-in-2025-protecting-modern-production-operations
[5] https://unit42.paloaltonetworks.com/iot-supply-chain/

Major Awareness Gaps Identified:

Fundamental Security Knowledge: Lack of staff security and awareness training are among the leading cybersecurity risks these days.

Risk Perception: Companies are entering a period where traditional cybersecurity approaches are increasingly inadequate against the evolving threat landscape, requiring fundamental changes in how organizations approach cyber resilience[6].

Sector-Specific Threats: Limited understanding of how cybersecurity threats specifically impact food safety, supply chain integrity and regulatory compliance requirements.

2.3 PRACTICE IMPLEMENTATION GAPS

Inconsistent Training Programs: Many small food sector organizations lack comprehensive, role-specific cybersecurity training that addresses both IT and OT environments.

Outdated Security Procedures: Organizations often operate with legacy security practices that do not account for modern threats like ransomware-as-a-service operations.

Cross-Functional Coordination: Poor integration between IT security teams and operational technology staff, creating blind spots in security coverage.

Vendor Management: Inadequate awareness of third-party risks and supply chain security requirements among procurement and operational teams.

2.4 TECHNICAL CAPABILITY GAPS

Skills Shortage: The food sector faces the same cybersecurity talent shortage as other industries, but with the added complexity of needing professionals who understand both traditional IT security and operational technology environments.

Legacy System Integration: Limited technical capabilities to secure aging industrial control systems and food processing equipment that was not designed with cybersecurity in mind.

Network Architecture: Many small organizations lack the technical expertise to properly segment networks between IT and OT environments, creating pathways for lateral movement during attacks.

Monitoring and Detection: Insufficient capabilities to monitor and detect threats across complex environments that include everything from farm sensors to processing plant controls.

Incident Response: Limited technical capabilities for rapid response to incidents that could affect food safety or production continuity.

2.5 SPECIALIZED FOOD SECTOR CONSIDERATIONS

Food Safety Integration: Understanding how cybersecurity incidents can directly impact food safety systems, traceability, and regulatory compliance.

Supply Chain Complexity: Limited awareness of cybersecurity risks across complex, multi-tier food supply chains involving numerous stakeholders.

Regulatory Compliance: Insufficient understanding of emerging cybersecurity regulations specific to the food sector and how they integrate with existing food safety requirements.

[6] https://www.weforum.org/stories/2025/02/biggest-cybersecurity-threats-2025/

Operational Continuity: Lack of awareness about how cybersecurity incidents can disrupt critical food production and distribution operations.

2.6 RECOMMENDATIONS FOR IMPROVEMENT

Sector-Specific Training: Develop cybersecurity awareness programs tailored to food sector operations, including scenarios involving food safety systems and supply chain disruptions.

Technical Capability Building: Invest in developing hybrid IT/OT security expertise within the workforce, potentially through partnerships with educational institutions.

Industry Collaboration: Leverage organizations like the Food and Agriculture Information Sharing and Analysis Center (Food and Ag-ISAC) to share threat intelligence and best practices. Currently, there is **no European-specific ISAC** focused purely on food/agriculture.

Integrated Approach: Adopt an integrated training model that merges cybersecurity awareness with food safety and HACCP training programs, ensuring a unified approach to risk management that reflects both regulatory and operational realities.

The food sector's unique combination of IT and OT environments, regulatory requirements, and public health responsibilities require specialized cybersecurity awareness approaches that address both traditional cyber threats and sector-specific vulnerabilities.

2.7 HOW AWARENESS CAN HELP CYBERSECURITY IN THE FOOD SECTOR

Human Firewall Development: Awareness training transforms employees into the first line of defence by helping them recognize and respond to social engineering attacks, phishing attempts, and suspicious activities that could compromise food safety systems.

Risk Recognition: Implementing robust cybersecurity practices, such as regular system updates, phishing awareness training, network segmentation, and secure data backups are critical for improving sector resilience. Awareness helps staff understand why these practices matter and how to implement them effectively.

Cultural Transformation: Building a security-conscious culture where cybersecurity becomes integrated into daily operations rather than an afterthought, particularly important given the sector's operational technology environment.

Incident Response Enhancement: Aware employees can identify and report potential security incidents faster, reducing dwell time and minimizing impact on food production and safety systems.

Relevance of cross-border coordination for transnational supply chains: The European food supply chain is highly interconnected, with materials, ingredients, and products crossing borders multiple times during production and distribution. A cyber incident affecting one entity can quickly cascade across the supply chain, causing disruptions to multiple businesses and potentially impacting food availability or safety. Effective cybersecurity necessitates robust mechanisms for international collaboration and the seamless exchange of threat intelligence across various national jurisdictions, ensuring a unified and proactive defence against evolving cyber risks. Such coordination is crucial for identifying and mitigating threats that may originate in one country but have consequences across the European Union.

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.

SECTION 3. TRAINING RESULTS

3.1 DELIVERY APPROACH ROMANIA

Romania is split into eight development regions, each with distinct economic characteristics:

- **Bucharest-Ilfov**: This is the most developed and urbanized region, characterized by the highest GDP per capita and a robust service sector. The engagement strategy here leveraged the region's advanced technological infrastructure and high digital literacy.
- **West**: As the second most developed and urbanized region, with a strong industrial base and a high employment rate, the training sessions stakeholders are likely to reflect the region's advanced industrial landscape and specific cybersecurity concerns.
- **Centre**: With a balanced mix of industries and services and high GDP per capita, the stakeholders acknowledge the interconnected nature of industry and service cybersecurity needs.
- **North-West:** The stakeholders from this region are characterized by dynamic economic growth, significant investment in industry and services, and robust business engagement.
- **North-East**: Since this is the least developed region with a significant rural population and lower GDP per capita, training programs should focus on understanding of cybersecurity principles and accessibility to digital security tools and guides.
- **South-East**: This region's economy includes a mix of agriculture, industry, and coastal fishing activities, influencing training content to reflect varied sector-specific cybersecurity requirements.
- **South-Muntenia**: Economically influenced by proximity to Bucharest, benefiting from spillover effects, particularly in services and industry.
- **South-West (Oltenia)**: To address challenges from lower GDP per capita and higher poverty rates, training sessions need to focus on accessible delivery methods and support materials for the stakeholders.

The training sessions, conducted from November 2024 to July 2025, were delivered online, by the DNSC team and Expertware team, using the Microsoft Teams platform complemented by interactive engagement through the platform Slido. This virtual approach ensured broad accessibility, efficient information dissemination, and real-time interaction despite geographic dispersion.

3.2 DELIVERY APPROACH BULGARIA

Bulgaria is divided into 6 (six) economic and statistical regions, which are used for the purposes of the regional planning, analysis, and allocation of European funding. They are not administrative units but play a significant role in the economic and social policy of the country.

The South-West region, dominated by the capital Sofia, is a major distribution and industrial production center in the food sector. Although primary agricultural production is relatively limited, it is home to large enterprise headquarters and logistics complexes that ensure efficient processing, packaging, and distribution of food. Sofia serves as a key market with high consumption and a place for innovation and high technologies in the food sector.

The South-Central region is one of the strongest food regions in Bulgaria, thanks to rich agricultural resources and developed industry in cities such as Plovdiv. Fruits, vegetables, meat, and dairy products are produced and processed here, with part of the production being exported outside the

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.

country. The presence of industrial zones and good transport infrastructure support the supply chain, allowing for rapid transportation and storage.

The North-eastern region includes Dobrudzha – one of the main grain-producing regions in the country, as well as Varna – an important port center. Mills, oil mills and dairy industries are developed here. Logistics plays a significant role, with the port of Varna facilitating exports, and internal transport links supporting the supply of producers with raw materials and the distribution of finished products.

The South-eastern region is known for the production of high-quality wines, especially in the areas around Yambol and Sliven. Stara Zagora is a center of energy and industrial processing of meat and dairy products. Burgas provides an important logistics platform through its port. The supply chain here is well developed, with the region oriented towards the export of wines, canned foods, and other products.

In the North-Central region, cities such as Ruse and Veliko Tarnovo are centers for the canning, meat, and dairy industries. This region is characterized by the presence of diverse primary production – from grain to fruits and vegetables. Danube transport through Ruse creates opportunities for access to international markets, although the region faces difficulties with demographic decline and aging infrastructure.

The North-western region is the least developed economic region in Bulgaria, and this is also reflected in the food sector. The main production here is concentrated in agriculture and livestock, but industrial processing is limited to small dairies and local producers.

The supply chain in the food sector in Bulgaria is extremely important for the successful functioning of the sector. Regional differences in primary production, processing and logistics determine the competitive advantages and weaknesses of each region. While the South-western and South-Central regions are leaders in terms of innovation and industrial production, the North-western region requires special attention and investment to improve the logistics network and production capacities.

3.3 TRAINING FOR MANAGEMENT OF ENTITIES ROMANIA

The training sessions targeted the management representatives from diverse subsectors within the food industry, with 71 participants attending. These participants came from key areas such as meat and poultry processing, seafood and dairy industries, grain milling and processing, oil and fat production, bakery, and beverage manufacturing, bottled drinking water supply, food packaging enterprises, and grocery retail, including supermarkets.

The training agenda was designed, by the DNSC team, to address specific cybersecurity responsibilities at the management level and provided a comprehensive understanding of the regulatory landscape under the NIS2 Directive. The core topics covered included an introduction to the NIS2 Directive and its transposition into national law, management and CISO roles, compliance obligations, and an interactive presentation of the CORB platform designed to enhance national and cross-border cooperation in cybersecurity.

Participants were also trained on best practices and strategic measures for cyber incident management relevant to managerial roles. To reinforce practical skills, the training incorporated a quiz type exercise aimed at preparing management teams for effectively handling cybersecurity incidents.

Regionally, Bucharest-Ilfov, being the most developed region, leveraged its advanced technological infrastructure and high digital literacy, attracting 21 participants.

Feedback from the participants was positive, with all responses rating the training highly. Participants notably appreciated the clarity of information provided and the practicality of the CORB platform demonstration. Additionally, feedback indicated it was particularly helpful for participants to clarify

the direction of NIS2 Directive implementation, fully understand the practical applicability of the NIS2 Directive, and gain a clear understanding of its specific requirements.

During the Q&A sessions, several questions were raised, particularly highlighting concerns around supply chain cybersecurity, including identifying necessary measures to ensure supply chain resilience. Participants also expressed interest in understanding the fines applicable to management under the NIS2 Directive and sought advice regarding further recommended trainings and courses for enhancing managerial cybersecurity competencies.

Valuable observations emerged from these sessions, including the importance of continuous management engagement and the need for periodic refresher sessions to maintain awareness and preparedness levels.

3.4 TRAINING FOR MANAGEMENT OF ENTITIES BULGARIA

In Bulgaria, the trainings for managers of food entities were 6 and were held during the period 26.06.2025 - 18.07.2025 entirely in an electronic environment, via the Webex platform. The total number of participants in the sessions was 83 people.

The main topics on the agenda of the trainings included:

- introduction to the NIS 2 Directive and its transposition into the national legislation,
- management roles and responsibilities in relation to compliance with the requirements,
- interactive presentation of the CORB platform, designed to support national and cross-border cooperation in the field of cybersecurity.
- present risks and threats in the cybersecurity. How can an organization be prepared for the NIS 2 Directive? Risk management and liability.
- practical training.

During the trainings, participants received information on good practices and strategic measures for responding to cyber incidents related to the responsibilities of management of the organization. To enhance practical skills, the training included a quiz-type exercise, published by the EU Survey platform, aimed at preparing managers for effective response to cybersecurity incidents.

During the sessions, participants were impressed by the level of sanctions applicable to managers under the NIS 2 Directive and sought advice on recommended training and courses to enhance management competencies in the field of cybersecurity.

The feedback from the participants was positive, with all highly appreciating the efforts made by the project team in training organizations in the sector. The participants appreciated the importance of the information provided and its practicality and were impressed by the prepared practical exercise. It was particularly useful for the participants to clarify their commitments in relation to the implementation of the NIS 2 Directive, to fully understand the practical applicability of that document and to gain a clear idea of its specific requirements for the management of the organization.

3.5 TRAINING FOR CYBERSECURITY STAFF ROMANIA

The training for cybersecurity staff gathered 80 participants representing various segments of the food sector, including meat and poultry processing, seafood and dairy industries, grain milling, oil and fat production, bakery and beverage manufacturing, bottled drinking water supply, food packaging companies, and grocery retailers and supermarkets.

The training sessions comprehensively covered key areas essential to cybersecurity staff, including their specific responsibilities and obligations within their roles, detailed methods for securing

operational technology (OT) and IT systems, practical insights into the NIS2 Directive requirements, technical controls, and compliance timelines. Participants were provided adoption guides, essential cybersecurity toolsets, and methodologies to enhance security throughout the supply chain. Additionally, a thorough demonstration of the CORB platform provided insights into self-enrolment of entities from the food sector and overall national and cross-border cooperation mechanisms.

Participant feedback was positive, with all nine responses emphasizing the practical nature of the training. Specifically, attendees highlighted the value of seeing the ongoing development of the NIS2 Directive reporting application, gaining current insights into Romania's cybersecurity landscape, and clarifying detailed NIS2 Directive requirements alongside best practices. Participants appreciated the straightforward guidance provided on protecting digital and operational infrastructure within the food sector, which increased their confidence in implementing effective cybersecurity controls aligned with Cyber Fundamentals Framework and the requirements derived from NIS2 Directive.

The feedback pointed out the importance and the impact of this training sessions, and the need for continuous awareness in cybersecurity.

3.6 TRAINING FOR CYBERSECURITY STAFF BULGARIA

The trainings for experts involved in the implementation of the NIS 2 Directive, as well as IT and cyber specialists, were held on-site in the respective planning region, as required by the project. The trainings were implemented during the period 03.07 – 16.07.2025 under the following schedule:

- For the North-western Planning Region – on 03.07.2025 from 13.00 to 15.00 - Vratsa, Hotel "Leva" (33 Georgi Benkovski Street), meeting room.
- For the South-western Planning Region – on 07.07.2025 from 10.30 to 12.30 - Sofia, Ministry of Electronic Governance (6 Gen. Gurko St.), meeting room on the ground floor
- For the North-eastern Planning Region – on 10.07.2025 from 2:30 p.m. to 4:30 p.m. - Varna, Regional Information Center-Varna (St. Cyril and Methodius Square (Kozirkata, Varna Center), meeting room
- For the North-Central Planning Region – on 11.07.2025 from 10.30 a.m. to 12.30 p.m. - Veliko Tarnovo, Municipal Administration Building (Mother Bulgaria Square No. 2), Ritual Hall
- For the South-Central Planning Region – on 15.07.2025 from 11.00 a.m. to 1.00 p.m. - Plovdiv, Boris Hristov Cultural Center (15 Gladstone Street), small conference room
- For the South-East Planning Region – on 16.07.2025 from 11.00 a.m. to 1.00 p.m. - Stara Zagora, Stara Zagora Municipal Administration Building (107 Tsar Simeon Veliki Blvd.), Slaveykov Hall.

A total of 91 participants from various sectors of the food industry, as well as public and non-governmental organizations, attended the on-site meetings.

The aim of the training was to examine the specific responsibilities of these cybersecurity professionals, as well as to ensure a comprehensive understanding of the regulatory framework introduced by the Directive on measures for a high common level of cybersecurity in the EU (NIS 2 Directive).

The trainings covered key aspects of the activities of cybersecurity specialists, with a focus on their specific responsibilities and obligations within their organizations.

The trainings program included:

• up-to-date information on the regulatory framework in cybersecurity.

• contemporary risks and threats in cybersecurity. How to prepare the entity for the NIS 2 Directive? Risk management and responsibilities of cybersecurity specialists.

• practical exercise for cybersecurity specialists.

Particular attention was paid to the CORB platform, through which participants received a detailed demonstration of the system's functionalities supporting national and cross-border cooperation in real time, including mechanisms for information exchange and incident response.

Regionally, the largest number of participants (22 people) in the trainings was in Stara Zagora (Southeastern planning region), followed by the city of Veliko Tarnovo for the North-Central region - 20 people.

Valuable observations were made as a result of these trainings, including the importance of the continuous engagement of IT and cyber specialists in the organization and the need to organize periodic trainings sessions to maintain their level of awareness and readiness to respond to incidents. The audience was reminded of the importance of sharing, reporting incidents within the required time frames, keeping backup copies of information from systems in an offline environment, and implementing two-factor protection for user access to these systems of the organization.

SECTION 4. OUTCOME AND IMPACT

4.1 OUTCOME AND IMPACT ROMANIA

The training sessions effectively engaged participants from diverse economic regions of Romania, reflecting varying degrees of regional interest and readiness regarding cybersecurity. The North-West region exhibited the highest overall engagement, suggesting a strong regional interest linked to a higher concentration of relevant cybersecurity entities. The Central region also showed robust participation, indicating substantial existing awareness and readiness for cybersecurity challenges.

Bucharest-Ilfov and the South region demonstrated moderate engagement, with cybersecurity staff participation slightly exceeding that of management, highlighting greater technical awareness or clearly identified cybersecurity roles at operational levels.

Conversely, regions such as South-East, South-West, and West exhibited notably lower participation rates, indicating potential areas for targeted outreach and support in future initiatives. These disparities underscore the need for tailored, region-specific strategies.

A significant positive outcome across most regions was the strong engagement of managerial personnel, reflecting heightened organizational commitment towards cybersecurity responsibilities mandated by the NIS2 Directive. This cross-role engagement promotes internal alignment, critical for effective cybersecurity governance and operational resilience.

The training significantly improved both strategic awareness and operational preparedness in cybersecurity among stakeholders across the food sector, fostering readiness for regulatory compliance and real-world incident response. The disparities observed between regions highlight critical areas for targeted follow-up actions, ensuring all regions benefit equally from future training initiatives.

To enhance future outcomes, targeted efforts should focus on underrepresented regions, leveraging successful strategies from high-engagement regions such as the North-West and Centre. Additionally, sustained and deeper technical training for cybersecurity staff should be prioritized, alongside mechanisms for ongoing support and post-training continuity.

The training sessions under the INFORB project reached stakeholders across all Romanian economic regions. Participants were divided into two main groups: **Management** and **Cybersecurity Staff** (cybersecurity officers or designated personnel). The graph demonstrates uneven distribution of participation by both region and role, offering insights into regional engagement and organizational role dynamics.

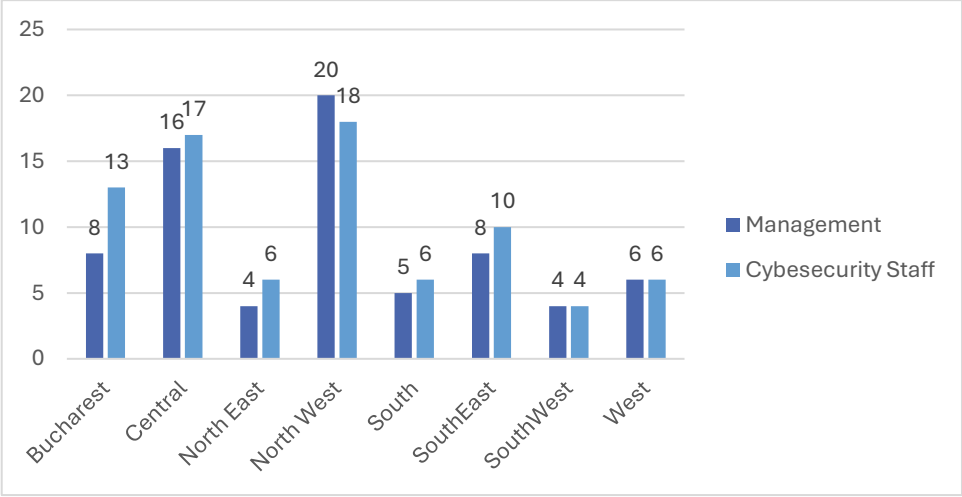

Figure 1. Distribution of the participants in the training sessions by economic region and target audience

Regional Distribution Insights

Highest Participation:

- **Highest Participation**: The North-West region had the highest participation for both target audiences (Management and Cybersecurity Staff), indicating strong regional engagement or a higher concentration of relevant entities in that region.
- **Strong Central Region Engagement**: The Central region closely follows, suggesting significant interest or existing awareness regarding cybersecurity training needs.

Moderate Participation:

- Bucharest-Ilfov region and South region show moderate attendance, with **Cybersecurity Staff** participation slightly higher than management in both.

Lower Engagement Regions:

- South-East, South-West, and West have noticeably lower attendance, with minimal variation between Management and **Cybersecurity Staff**. These areas may require targeted outreach or further support in future initiatives.

Target Audience Engagement:

- Across most regions, the Management audience either matched or exceeded **Cybersecurity Staff** participation. This indicates a positive outcome: leadership within food sector entities is engaging with cybersecurity and regulatory responsibilities.
- However, in regions like Bucharest-Ilfov and South, **Cybersecurity Staff** attendance exceeded management, reflecting either greater technical awareness or better identification of cybersecurity roles at the operational level.
- Considering high engagement regions (North-West, Central), leveraging successful outreach strategies and training methods used here might increase participation in lower-engagement regions.

Observed Impacts:

- **Awareness Raised:** The participation of both strategic and operational roles confirms improved awareness of the food sector's cybersecurity responsibilities under NIS2.
- **Regional Variability:** Disparities in participation highlight the need for region-specific strategies, especially in lower-engagement areas where critical infrastructure may still lack sufficient exposure to these issues.
- **Cross-role Communication:** The involvement of both managers and technical personnel fosters internal alignment, which is essential for effective cyber risk governance.

Implications for Future Actions:

- **Focus on Underrepresented Regions:** Future training sessions should prioritize South-West, West, and South-East, potentially through local partnerships, chambers of commerce, government or industry associations.
- **Deeper Engagement of Cybersecurity Staff Roles:** Although Cybersecurity Staff participation was consistent, it should be expanded with more technical content and follow-up opportunities, especially in regions where management engagement is already strong.

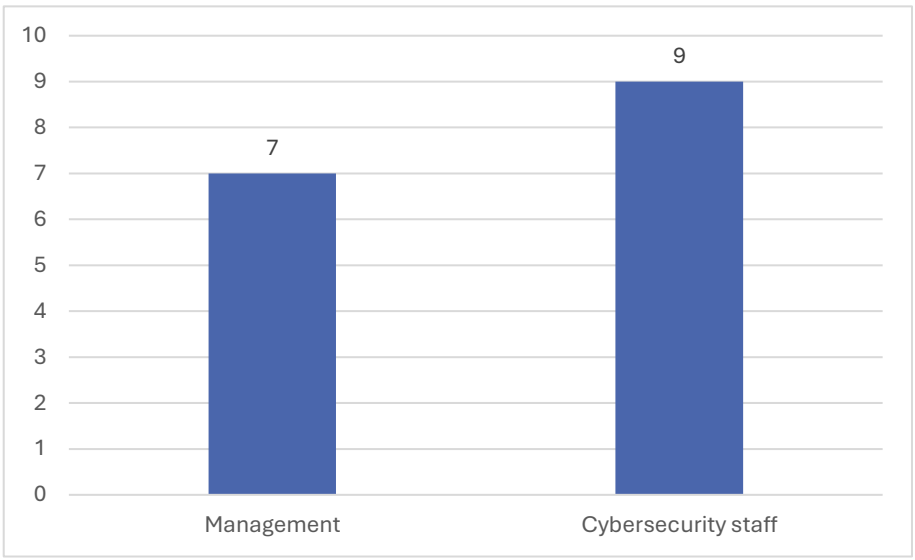

Figure 2. Number of feedback surveys filled out by the target audience

Post-Training Continuity: Entities that participated actively, especially in North-West and Central regions, could be recruited as ambassadors or mentors to promote best practices within their networks. The feedback survey, published with the help of the EU Survey platform, indicates a marginally higher engagement level or responsiveness among cybersecurity professionals concerning feedback activities. It could also reflect a greater interest in continuous improvement and technical detail among the cybersecurity staff group, emphasizing their proactive stance towards cybersecurity training outcomes and relevance. For future training sessions, enhancing efforts to encourage management to provide feedback could help balance insights from both strategic and operational perspectives.

4.2 OUTCOME AND IMPACT BULGARIA

The training initiatives successfully engaged stakeholders from diverse economic regions of Bulgaria, highlighting both regional strengths and gaps in cybersecurity readiness across the food sector. The South-East region showed the highest overall engagement, suggesting strong regional interest. The North-Central region also showed robust participation, indicating significant existing awareness and readiness to address cybersecurity challenges.

The remaining regions, such as South-West and South-Central, demonstrated lower participation rates, and are suggesting potential areas for targeted outreach and support in future initiatives.

A significant positive outcome in most regions was the strong engagement of both – the managers and the cybersecurity experts, reflecting the increased organizational commitment to cybersecurity responsibilities assigned by the NIS 2 Directive. This engagement encourages the organization to comply with regulatory requirements, which is crucial for effective cybersecurity management and ensures operational sustainability.

The trainings effectively raised awareness of contemporary cybersecurity risks and threats and responsibilities facing food entities, with participants seeing progress in both strategic understanding and practical implementation capabilities. The observed differences between regions highlight critical areas for targeted future action, ensuring that all regions will benefit equally from future training initiatives.

In order to improve future results, targeted efforts must be focused on underrepresented regions, such as the North-West and North-East planning regions. In addition, it is necessary to prioritize regular training of personnel in the field of cybersecurity, as well as mechanisms for ongoing support and continuity after training.

The training sessions under the INFORB project reached stakeholders in all Bulgarian economic development regions. The participants were divided into two main groups: management team and specialists in cybersecurity and in implementing the requirements of the NIS 2 Directive and the Cybersecurity Act. The graph demonstrates the uneven distribution of participation by region, based on the number of participants in the trainings on site.

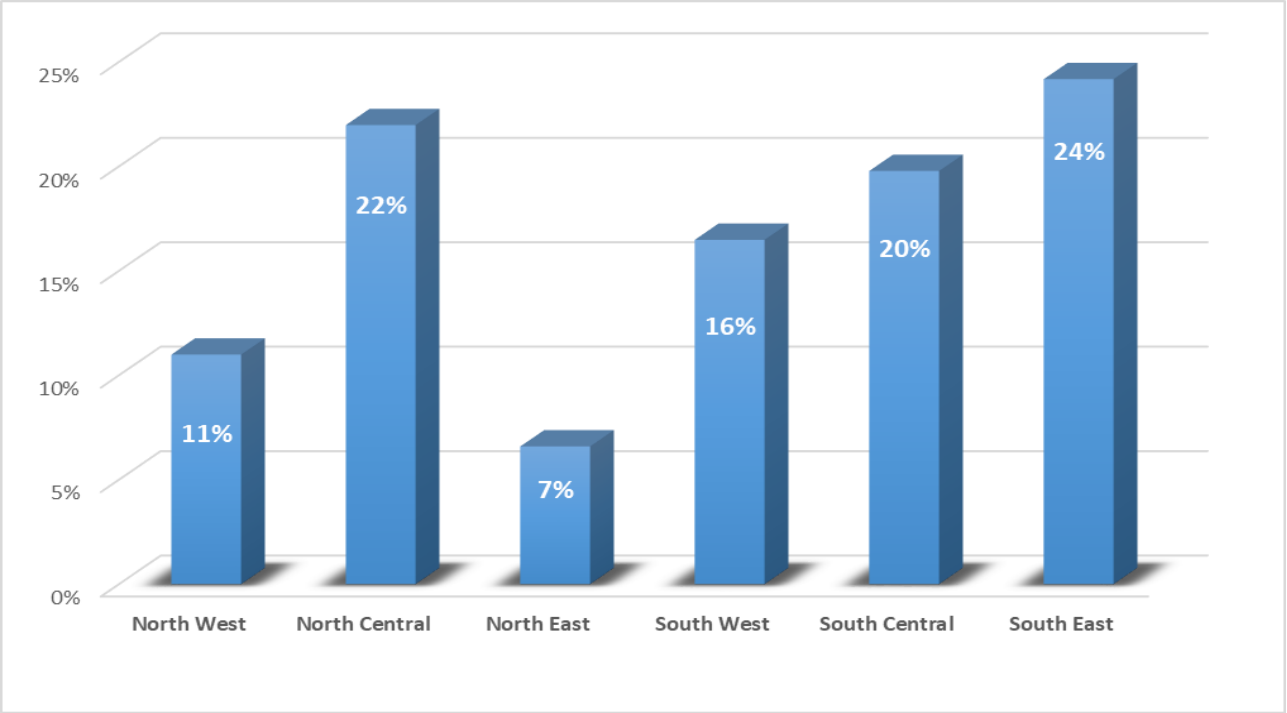

Figure 3.Distribution of the participants in the on-site training sessions by economic region

Regional Distribution Data:

1. **Highest Participation:**

• **Highest Participation:** The Northeast region had the highest participation, indicating strong regional engagement and a higher concentration of stakeholders from the sector.

• **Strong North-Central Region Engagement**: The North-Central region demonstrated significant interest or better awareness of cybersecurity training needs.

2. **Medium Participation:**

• **South-Central and South-West regions** demonstrated moderate attendance.

3. **Lower Engagement Regions:**

• **North-West and North-East regions** had significantly lower attendance. These areas may require targeted outreach or additional support in future initiatives.

Target Audience Engagement:

• In the most regions, the audience was mixed, with both management and cybersecurity experts and other relevant stakeholders in the organization. This demonstrates a positive outcome of the team's efforts: employees in food entities are engaged with cybersecurity and with the regulatory requirements in the field.

• Considering regions with important levels of participation/engagement (North-East, North-Central), the use of more trainings can increase the interest in participation within the regions with lower levels of engagement.

Observed impacts:

• **Awareness raising:** The participation of both strategic and operational players confirms the improved awareness of the food sector's cybersecurity responsibilities within the NIS 2.

• **Regional variability**: The differences in participation highlight the need for region-specific strategies, especially in areas with lower levels of engagement, where critical infrastructure may still be under-exposed to these issues.

• **Cross-role communication**: Involving both management and technical staff promotes internal alignment, which is essential for effective cyber risk management.

Implications for future actions:

• **Focus on underrepresented regions:** Future training sessions should prioritize the North-East and North-West regions, through local partnerships, chambers of commerce, government or industry associations.

• **Deeper staff engagement in cybersecurity**: While staff engagement in cybersecurity was consistent, the trainings should be expanded with more technical content and follow-up opportunities, especially in regions where management engagement is already strong.

• **Continuity after training:** Organizations that have actively participated, especially in the North East and North Central, could be appointed as ambassadors to promote good practices within their organizations.

SECTION 5. STRATEGIC INSIGHTS AND RECOMMENDATIONS

5.1 STRATEGIC INSIGHTS ROMANIA

The analysis of participation data and stakeholder feedback from the INFORB training sessions provides valuable insight into the current state of cybersecurity awareness and preparedness in the food sector. This data offers key insights and helps us form recommendations for helping the food sector achieve resilience and good cybersecurity posture.
This chapter outlines key strategic insights derived from the training outcomes and proposes targeted recommendations to enhance the impact and sustainability of cybersecurity capacity-building in the food sector.

Management Engagement Is Critical and Achievable:

- Strong management participation in specific regions (e.g., North-West, Central) shows that executive-level stakeholders recognize their accountability under the NIS2 Directive.
- However, variation across regions reveals that not all leadership teams are equally aware or prepared, strategic messaging and incentives matter.

Regional Disparities Signal Uneven Cyber Readiness:

- Regions like South-West, South-East, and West had the lowest participation. This could reflect limited local awareness, fewer large food enterprises, or logistical access issues.
- These areas may be more vulnerable due to lack of preparedness and would benefit from targeted support.

Cybersecurity Roles Need Deeper and Ongoing Support:

- Cybersecurity staff participation was moderate, while this is expected given their lower numbers in organizations, it may indicate a lack of structured cybersecurity responsibilities at the operational level.
- Many entities, from the food sector, rely on IT generalists or external providers, which weakens institutional continuity and preparedness.

Cross-role Participation Lays a Foundation for Internal Alignment:

- Where both management and cybersecurity staff were represented (e.g., Central, North-West), organizations are better positioned to implement a unified cybersecurity strategy and establish an Information Sharing and Analysis Center (ISAC) to enhance threat intelligence and collaborative defence capabilities.
- This dual engagement is a prerequisite for building a culture of cyber responsibility that goes beyond compliance.

5.2 STRATEGIC INSIGHTS BULGARIA

The analysis of stakeholder participation and feedback data from the INFORB training sessions provides valuable information at the national level on the current state of cybersecurity awareness and preparedness in the food sector. This data provides key information and helps to formulate recommendations to help the food sector achieve resilience and a good cybersecurity posture.

This section outlines key strategic conclusions arising from the training results and offers targeted recommendations to increase the impact and sustainability of cybersecurity capacity building in the food sector.

Leadership engagement is critical and achievable:

• Stakeholders in management positions recognize their responsibility under the NIS 2 Directive.

• The lack of great participation of entities in the training, or lack of feedback from managers of important enterprises for the sector, demonstrates the lack of sufficient public awareness on the topic of future commitments concerning them following the adoption by the National Assembly of the Act on Amendments of the Cybersecurity Act.

Cybersecurity roles need deeper and more sustained support:

• Given the small total number of participants in the events based on the total number of registered food entities in the country may indicate a lack of structured cybersecurity responsibilities at the operational level.

• Many organizations are likely to rely on IT/cyber specialists or external providers, which reduces institutional continuity and preparedness for incident response.

5.3 RECOMMENDATIONS FOR ROMANIA

Expand Targeted Outreach in Low-Engagement Regions:

- Prioritize **South-East, South-West, and West** with follow-up campaigns and localized workshops.
- Engage regional business associations, food industry clusters, and agricultural cooperatives to mobilize participants.

Institutionalize Cybersecurity Training for Both Roles:

- Establish periodic awareness sessions for **management** (e.g., yearly briefings, incident simulation exercises).
- Develop a dedicated capacity-building pathway for **cybersecurity staff**, with practical guidance, technical webinars, and community support channels.

Encourage Role Definition Within Entities:

- Support food sector organizations in formally designating **cybersecurity officers or focal points**, especially in small and medium-sized enterprises.
- Provide role descriptions, minimum expectations, and template policies through the CORB platform.

Leverage High-Engagement Regions as Peer Support Hubs:

- Use active participants from regions like **North-West and Central** to mentor or advise less-engaged areas.
- Promote peer learning through success stories, cross-region panels, or digital knowledge exchange via CORB.

Integrate Cybersecurity into Broader Sector Risk Management:

- Frame cybersecurity as part of food safety, quality assurance, and business continuity to resonate more with sector leaders.
- Include it in certifications, audits, and supplier evaluations to embed responsibility across the supply chain.

Use CORB Platform to Maintain Engagement and Reporting:

- Encourage regular use of CORB for sharing incidents, good practices, and updates on regulatory compliance.

- Develop a **cybersecurity bulletin or dashboard** within CORB for food sector entities, including alerts, legal updates, and case studies.

Strengthen Collaboration with Academic and Research Institutions:

- Establish formal partnerships with universities and cybersecurity research centers to co-develop training curricula, facilitate access to expert resources, and promote sector-specific research on cyber threats and digital resilience in the food industry.

5.4. RECOMMENDATIONS FOR BULGARIA

Expanding the target coverage in regions with low engagement:

- Prioritizing the North-East and North-West regions with follow-up awareness campaigns and local seminars/trainings.
- Engaging regional business associations, clusters, hubs and other food sector organizations to mobilize participants in events and trainings.

Institutionalizing cybersecurity training for both roles:

- Establishing periodic awareness-raising sessions for managers (e.g. annual meetings, incident simulation exercises).
- Supporting capacity building for IT and cyber professionals with practical guidance, technical webinars and online support channels.

Using high engagement regions as hubs for peer support:

- Using participants from active regions as ambassadors of cybersecurity good practices.
- Promoting peer-to-peer exchange of experience, including through the online platform developed under the project.

Integrate cybersecurity into risk management in the wider sector:

- Involvement in supplier certification, audits and assessments to take responsibility across the supply chain.

Use the CORB online platform to maintain engagement and reporting:

- Encourage regular use of CORB to share incidents, good practices and up-to-date information on regulatory compliance.
- Develop a CORB cybersecurity bulletin or dashboard for food sector entities, including alerts, legal updates and case studies.

Establish an appropriate legal framework tailored to the specific cybersecurity needs of the food sector:

- Accelerate the transposition of the NIS 2 Directive into national legislation, through the adoption of the Law on Amendments and Supplements to the Cybersecurity Act.
- Issue clear instructions/manuals/guidelines to the food sector regarding its alignment with the requirements of the updated cybersecurity framework.

* * *

The official version of the Document is in English, while at the national level, in Romania and Bulgaria, it will be published in the official languages of these countries, namely Romanian and Bulgarian.