EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CYBERSECURITY ROLES AND SKILLS FOR NIS2 ESSENTIAL AND IMPORTANT ENTITIES

Mapping NIS2 obligations to ECSF

JUNE 2025

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For contacting the authors, please use euskills@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

Konstantinos ADAMOS, University of the Aegean
Fabio DI FRANCO, ENISA
Sozon LEVENTOPOULOS, Athens University of Economics and Business

ACKNOWLEDGEMENTS

George Stergiopoulos, University of the Aegean

LEGAL NOTICE

This publication represents the views and interpretations of ENISA, unless stated otherwise. It does not endorse a regulatory obligation of ENISA or of ENISA bodies pursuant to the Regulation (EU) No 2019/881.

ENISA has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only and it must be accessible free of charge. All references to it or its use as a whole or partially must contain ENISA as its source.

Third-party sources are quoted as appropriate. ENISA is not responsible or liable for the content of the external sources including external websites referenced in this publication.

Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

ENISA maintains its intellectual property rights in relation to this publication.

COPYRIGHT NOTICE

ISBN 978-92-9204-706-1, doi: 10.2824/8870995

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The national transpositions of the NIS2 Directive[1] are going to affect tens of thousands of entities[2] across the European Union (EU), many of which are facing new legal requirements for the first time and will need to address new staffing needs to ensure compliance[3].

For organisations — especially medium sized enterprises — translating legal requirements into clear tasks for their workforce is a major challenge. They are asking questions such as the following:

- **Which roles and skills are needed to meet these requirements?**
- **Which step-by-step approach can guide my organisation in implementing the necessary organisational, workforce, and strategic planning?**

For EU Member States, ensuring compliance with the NIS2 Directive is not just about drafting legislation — it's important to set up the right conditions so these laws can be put into practice effectively. Competent authorities must translate regulatory obligations into clear policies, capacity-building initiatives, and workforce strategies that empower both the public and private sectors to meet cybersecurity requirements.

To help overcome these challenges, ENISA in line with articles 6 and 10 of the Cybersecurity Act[4], prepared this guidance document on the skills and roles for the cybersecurity professionals needed to meet these legal requirements effectively. The guidance is based on the European Cybersecurity Skills Framework (ECSF)[5], the EU's reference framework for defining and assessing cybersecurity skills for professionals as mentioned in the Communication on the Cybersecurity Skills Academy[6].

This guidance presents a detailed mapping between the obligations outlined in the NIS2 Directive and the ECSF role profiles. It focuses exclusively on essential and important entities covered by the directive. Each role is mapped to its specific tasks, assisting entities in understanding what personnel capabilities are required to fulfil these obligations successfully. The detailed connections aim to guide entities in deploying the right team members to adhere to these standards.

Additionally, this guidance acts as a valuable resource for Member States, assisting them in evaluating and improving the cybersecurity preparedness of essential and important entities. It clarifies key deliverables, highlights opportunities for cross-role collaboration, and ensures that

[1] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance) (OJ L 194, 19.7.2016, pp. 1–30, ELI: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[2] Compared to NIS1, the NIS2 Directive introduces several new sectors, including waste water, space, public administration, ICT service management (business-to-business), postal and courier services, and waste management, among others — bringing the total to 18 sectors across essential and important entities. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[3] According to ENISA's NIS Investments 2024 report, a significant 89% of surveyed organisations reported that they will require additional cybersecurity staff to comply with NIS 2. https://www.enisa.europa.eu/publications/nis-investments-2024

[4] Cybersecurity Act of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, pp. 15–69, ELI: https://eur-lex.europa.eu/eli/reg/2019/881/oj

[5] ENISA (2022): https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf

[6] Communication from the Commission to the European Parliament and the Council – Closing the cybersecurity talent gap to boost the EU's competitiveness, growth and resilience ('The Cybersecurity Skills Academy'), COM(2023/207) final of 18 April 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023DC0207

cybersecurity skills are strategically aligned with the NIS2 Directive's risk management, incident responding and reporting requirements.

At its core, this initiative supports the vision of a secure and resilient Europe, where a skilled and well-prepared cybersecurity workforce plays a vital role in maintaining regulatory compliance and operational strength. In an era of increasingly complex threats, this effort is a step toward building a trusted and cyber-secure future for the EU.

DISCLAIMER

This document is intended as a practical guide and is not legally binding. It offers advisory support and does not replace any legal frameworks, guidance, or procedures established under Member States' national law. Entities falling under the scope of the NIS2 Directive should always consult their respective national competent authorities and follow the official guidance provided at the national level.

This practical guide can serve as a useful resource for both entities and Member States. It offers a structured view of how NIS2 obligations may align with cybersecurity roles and tasks as described in the European Cybersecurity Skills Framework (ECSF), along with examples of how essential and important entities can make use of this mapping when planning staffing, upskilling, reskilling, or outsourcing. National authorities may also find it helpful when shaping their own strategies or support materials for implementation.

1. INTRODUCTION

The NIS2 Directive marks a significant step in enhancing cybersecurity across the European Union. It provides a clear and comprehensive approach to managing cyber risks, reporting incidents, and sharing information. The directive introduces enhanced security requirements for essential and important entities, while also reinforcing the supervisory responsibilities of national competent authorities. However, enhancing cybersecurity extends beyond policy — it requires the effective engagement of people. To implement the directive effectively, entities should define internal cybersecurity roles and responsibilities aligned with its requirements[7].

A major challenge to meeting NIS2 requirements is linking regulatory obligations to practical implementations. The ECSF, developed and maintained by ENISA, plays a pivotal role in this process, offering a practical tool to define and communicate the roles and skills necessary for cybersecurity professionals. The ECSF maps twelve (12) distinct cybersecurity role profiles[8], which are integral to meeting the obligations of the directive, such as risk management, incident response and reporting.

A practical guide to help leaders and organisations translate NIS2 obligations into clear and actionable tasks

This document serves as a practical guide to help leaders and organisations turn NIS2 obligations into real actions. Linking these obligations to ECSF role profiles offers a structured pathway for:

- **Policymakers and national authorities** to boost their national cybersecurity strategies, prioritise resources, and build the cybersecurity capabilities to meet legal requirements.
- **Essential and important entities** to understand how NIS2 obligations translate to specific workforce responsibilities. This helps them recruit, provide training, or outsource.

To achieve these objectives, the document includes a detailed mapping of NIS2 obligations to relevant ECSF role profiles along with practical use cases to support the implementation of the directive.

This helps entities of all sizes use their resources effectively and build cybersecurity teams capable of handling NIS2 obligations. By combining regulatory demands with workforce development, this guide supports all stakeholders in creating a strong, adaptable, and future-ready cyber-resilient environment across the EU.

1.1 PURPOSE AND TARGET AUDIENCE

1.1.1 Purpose

This document is a practical guide to translating NIS2 obligations into concrete actions for policymakers and entities. Leveraging the ECSF provides a structured approach to workforce alignment, capacity building and strategic cybersecurity planning.

Specifically, this document aims to:

- **Support Member States** in developing their cybersecurity strategies, prioritising their resources and building cybersecurity capabilities to meet NIS2 requirements.

[7] NIS 2 Directive does not apply directly to entities in scope of the directive. Instead, it sets objectives that must be transposed into national law. The obligations for entities arise from these national measures, which are required to achieve the goals set out in the Directive.

[8] European Cybersecurity Skills Framework Role Profiles (2022): https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles

- **Guide Essential and Important Entities** in understanding how legal requirements translate into operational tasks, so they can build their cybersecurity teams through hiring, reskilling, upskilling, or outsourcing.

By aligning regulatory requirements with organisational capabilities and workforce capacities this document enables organisations and policymakers to build a more cyber resilient landscape in the EU.

1.1.2 Target Audience

- **Competent and Legislative Authorities:** National and EU-level policymakers looking to strengthen their cybersecurity frameworks by integrating NIS2 into their strategies, policies and capacity-building initiatives.
- **Essential and Important Entities:** Organisations affected by NIS2 that need to translate regulatory requirements into structured workforce roles, refine job descriptions and decide whether to implement targeted learning and development programmes to upskill their workforce or outsource some of the tasks.

This document is the bridge between legislation and implementation, providing tailored solutions to help stakeholders meet NIS2 requirements while building cybersecurity resilience.

1.2 DOCUMENT STRUCTURE

This document serves as an easy-to-follow guide for organisations and policymakers. It aims to help them align their cybersecurity teams with the NIS2 requirements by using the ECSF. Each section covers the following topics:

- **Section 2** highlights several obligations set out in relevant NIS2 articles, providing a clear understanding of what is required.
- **Section 3** demonstrates these duties with practical examples. It shows how a medium-sized organisation, with limited resources, can use ECSF role mapping to increase their cybersecurity posture and on doing so, work towards the implementation of the NIS2 obligations.
- **Section 4** contains the comprehensive mapping of roles - detailing the responsibilities, tasks, expected outcomes, and potential collaborations for each ECSF role profile - to NIS2 Directive requirements. It also highlights the benefits of this mapping, demonstrating how this approach enhances clarity, efficiency, and workforce planning.
- **Annex I** presents the methodology behind the mapping process, detailing how NIS2 obligations were systematically linked to ECSF role profiles.

2. NIS2 OBLIGATIONS

This section introduces two articles of the NIS2 Directive, which outline several obligations for entities falling within its scope. Article 21 states that essential and important entities must apply proper cybersecurity risk management steps. This covers areas like dealing with incidents, securing the supply chain, and maintaining smooth business operations. Article 23 highlights the duty of these entities to report incidents. They must inform their competent authorities and/or Computer Security Incident Response Teams (CSIRTs) on time about any significant incidents. To support compliance and facilitate coordinated responses, it is important to define responsibilities related to each obligation. Each task from the NIS2 Directive is linked to specific ECSF role profiles as presented in Section 4.

2.1 ARTICLE 21: CYBERSECURITY RISK-MANAGEMENT MEASURES

1. Member States shall ensure that essential and important entities **take appropriate and proportionate technical, operational and organisational measures to manage the risks posed** to the security of network and information systems which those entities use for their operations or for the provision of their services and to prevent or minimise the impact of incidents on recipients of their services and on other services.

Taking into account the state-of-the-art and, where applicable, relevant European and international standards, along with the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. **When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of incidents occurring and their severity, including their societal and economic impact**.

2. The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

a) policies on risk analysis and information system security;
b) incident handling;
c) business continuity, such as backup management and disaster recovery, and crisis management;
d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
g) basic cyber hygiene practices and cybersecurity training;
h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;
i) human resources security, access control policies and asset management;
j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

2.2 ARTICLE 23: REPORTING OBLIGATIONS

1. Each Member State shall ensure that essential and important entities **notify**, without undue delay, its CSIRT or, where applicable, its competent authority in accordance with paragraph 4 of **any incident that has a significant impact on the provision of their services as referred to in paragraph 3 (significant incident)**. Where appropriate, entities concerned shall **notify, without undue delay, the recipients of their services of significant incidents that are likely to adversely affect the provision of those services**. Each Member State shall ensure that those entities report, inter alia, any information enabling the CSIRT or, where applicable, the competent authority to determine any cross-border impact of the incident. The mere act of notification shall not, in itself, subject the notifying entity to increased liability.

Where the entities concerned notify the competent authority of a significant incident under the first subparagraph, the Member State shall ensure that the competent authority forwards the notification to the CSIRT upon receipt.

In the case of a cross-border or cross-sectoral significant incident, Member States shall ensure that their single points of contact are provided in due time with relevant information notified in accordance with paragraph 4.

2. Where applicable, Member States shall ensure that **essential and important entities communicate, without undue delay, to the recipients of their services that are potentially affected by a significant cyber threat any measures or remedies that those recipients are able to take in response to that threat**. Where appropriate, the entities shall also inform those recipients of the significant cyber threat itself.

3. An incident shall be considered to be significant if:

a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;
b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

4. Member States shall ensure that, for the purpose of notification under paragraph 1, the entities concerned submit to the CSIRT or, where applicable, the competent authority:

a) without undue delay and in any event within 24 hours of becoming aware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;
b) without undue delay and in any event within 72 hours of becoming aware of the significant incident, an incident notification, which, where applicable, shall update the information referred to in point (a) and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise;
c) upon the request of a CSIRT or, where applicable, the competent authority, an intermediate report on relevant status updates;
d) a final report not later than one month after the submission of the incident notification under point (b), including the following:
(i) a detailed description of the incident, including its severity and impact;
(ii) the type of threat or root cause that is likely to have triggered the incident;
(iii) applied and ongoing mitigation measures;
(iv) where applicable, the cross-border impact of the incident;
(v) in the event of an ongoing incident at the time of the submission of the final report referred to in point (d), Member States shall ensure that entities concerned provide a progress report at that time and a final report within one month of their handling of the incident.

By way of derogation from the first subparagraph, point (b), a trust service provider shall, with regard to significant incidents that have an impact on the provision of its trust services**, notify the CSIRT or, where applicable, the competent authority, without undue delay and in any event within 24 hours of becoming aware of the significant incident**.

3. USE CASES

To make the NIS2 obligations and their mapping to ECSF role profiles more accessible and understandable for entities, the following sections present two scenarios illustrating how the ECSF can be leveraged to enhance cybersecurity maturity. Both scenarios are based on a **medium-sized organisation** with limited financial and human resources, characterised by **informal, decentralised cybersecurity governance** and a **low maturity level**. It is important to note, however, that this is not a one-size-fits-all approach. Every organization has a unique approach towards cybersecurity, and the implementation should be tailored accordingly, using the detailed mapping provided in Section 4 of this document.

The first scenario outlines how the ECSF can be leveraged for NIS2 implementation efforts, while the second focuses on post-incident reporting in line with Article 23. These use cases demonstrate how entities within the scope of NIS2 directive can utilize the ECSF to support strategic workforce planning and organizational development, ultimately enhancing their cybersecurity posture and resilience.

TAILORED APPLICATION

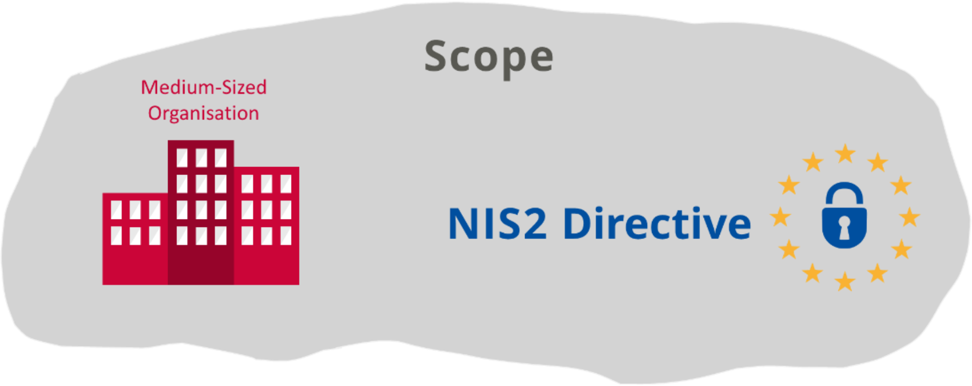
The use case provided can be adjusted based on the detailed mapping of Section 4, considering the organisation's size, structure, operational needs, and available resources to ensure a practical and realistic application of NIS2 obligations.

3.1 SCENARIO 1: NIS2 IMPLEMENTATION OF CYBERSECURITY RISK MEASURES

3.1.1 Introduction

Until now, the medium-sized organisation in this scenario has managed its cybersecurity in an informal, decentralized manner, addressing challenges on an ad-hoc, case-by-case basis. However, with the implementation of the NIS2 Directive into national legislation, many organisations—including this one—now fall under its regulatory scope, requiring a more structured and proactive approach to cybersecurity.

Figure 1: A Medium-Sized Organisation in scope of the NIS2 Directive

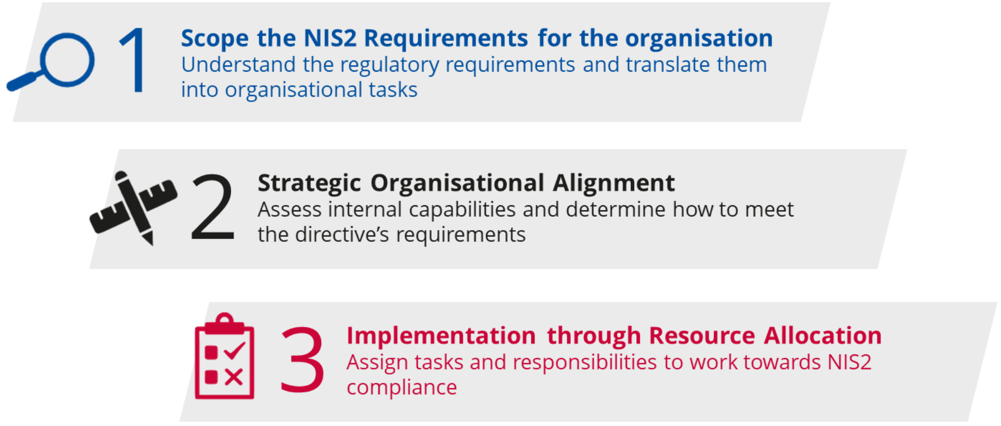


The organisation's management sought practical guidance to implement the cybersecurity risk management measures[9]. They recognized that the European Cybersecurity Skills Framework (ECSF) could help them identify and address organisational capability gaps—whether through upskilling, reskilling, hiring, or procuring external services. In fact, the ECSF can serve as foundational tool for the development of the roles, responsibilities and competences. With the

[9] IMPLEMENTATION GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555

roadmap illustrated in Figure 2, the organisation now has a **clear and actionable starting point**.

Figure 2: Roadmap to NIS2 implementation



1 **Scope the NIS2 Requirements for the organisation**
Understand the regulatory requirements and translate them into organisational tasks

2 **Strategic Organisational Alignment**
Assess internal capabilities and determine how to meet the directive's requirements

3 **Implementation through Resource Allocation**
Assign tasks and responsibilities to work towards NIS2 compliance

3.1.2 Organisational Tasks

Through collaboration with an industry network, the organisation identified the following organisational tasks as necessary to establish a cybersecurity baseline and ensure compliance.

Organisational tasks
1. Define and implement cybersecurity plans and policies
Develop strategies and policies to comply with cybersecurity regulations.
Oversee the cybersecurity policy and assign responsibilities to implement measures and fulfil reporting obligations.
Manage relationships with suppliers and ensure their security to protect the supply chain.
Regularly update the management board on cybersecurity plans and strategies.
Create plans to ensure the business can continue operating and recover quickly in case of a disaster.
2. Manage the cybersecurity risk
Develop and apply policies for risk analysis, system security, supplier security, encryption, access control, asset management, and HR security.
Teach management about cybersecurity risks, threats, and their impact on the organisation.
Inform management about cybersecurity risk management measures.
3. Collaborate with authorities and other stakeholders
Share information and provide reports to authorities and other interested parties.
Ensure compliance with binding instructions or orders from authorities.
4. Ensure compliance through cybersecurity audits
Conduct independent reviews of information and network security of the organisation.
Conduct internal audits and provide reports to authorities when requested.

5. Oversee and assure compliance with the Directive
Make sure the organisation follows data protection laws (NIS2 and GDPR) when handling personal data.
Submit required information to authorities to get listed as an essential entity and update them about any changes.
Ensure proper handling and access to domain name registration data by relevant entities.
6. Inform stakeholders regarding compliance obligations
Tell management they are responsible for approving cybersecurity measures and must complete cybersecurity training.
Ensure top management knows if they need to appoint a representative for companies not based in the EU but offering services there.
7. Plan, design, and implement security solutions and controls
Plan and build secure networks and ensure a secure environment. .
Implement strong security features like multi-factor authentication (MFA), and secure communications for voice, video, text, and emergencies.
Develop, set up, manage, and monitor cybersecurity measures such as secure network configurations and system integrations.
Apply cybersecurity measures and safeguards based on the risk management results and planning, and address issues identified during the audits.
8. Deliver cybersecurity training
Create and deliver appropriate cybersecurity training programmes aimed at members of management bodies of entities and their employees.
Implement basic cyber hygiene practices and designs and deliver cybersecurity training.
9. Collect and analyse information to identify threats
Collect and analyse cyber threats, then create reports and share them with relevant parties.
Oversee the process of collecting, analysing, and sharing cybersecurity information, including threats, near misses, vulnerabilities, and attack techniques.
10. Ensure effective response and reporting of cybersecurity incidents
Develop and establish a plan for responding to cybersecurity incidents.
Evaluate and report any vulnerabilities to the Computer Security Incident Response Team (CSIRT).
Manage cybersecurity incidents and disclose any vulnerabilities found.
Identify, analyse, and report cybersecurity incidents to CSIRTs, authorities, and service recipients.
11. Conduct security assessment tests
Conducts penetration tests and vulnerability assessments to assess the effectiveness of cybersecurity solutions and provides, when requested, the vulnerability assessment and/or penetration testing reports to the competent authorities. Plan and continuous perform security tests (including but not limited to penetration tests and vulnerability assessments) as per the results of the risk management process. Document the findings and apply appropriate mitigating actions in case of critical findings.
Assists the competent authorities' personnel on the security scans conducted.

3.1.3 Strategical organisational alignment and Resource allocation

To effectively address the organisational tasks detailed in the previous section, strengthen governance, and meet the need for specialised skills in specific areas, the senior management, decided to establish clear internal accountability and to engage targeted expertise through outsourcing. Based on this approach, the following steps were implemented.

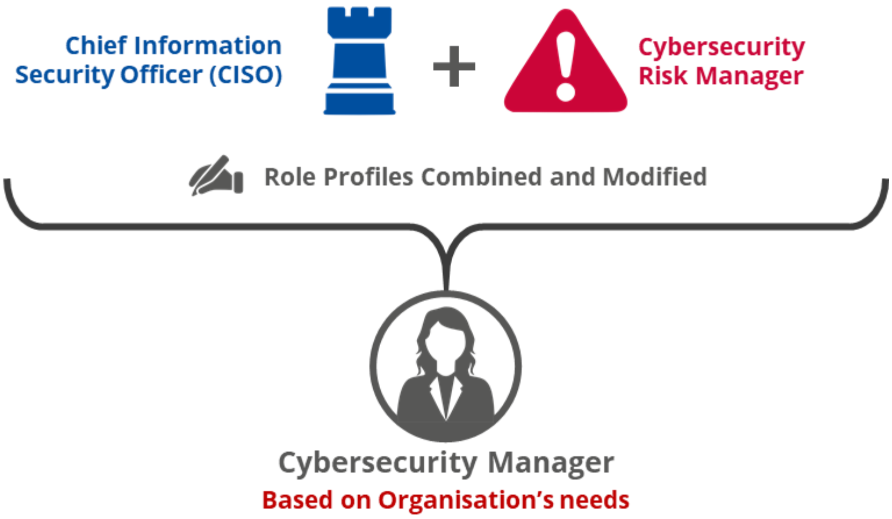
Step 1: Hire a Cybersecurity Manager

As a first step to address tasks **1, 2, and 3**, the senior management decided to appoint a cybersecurity manager responsible for developing the organisation's policy on the security of network and information systems, as well as topic-specific policies, procedures, processes, and plans to establish a security baseline.

This role is expected to provide strategic oversight of the entity's cybersecurity programme, underlining the senior management's commitment to cybersecurity. Given the size of the organisation, the role should also encompass responsibility for managing cybersecurity risks, including the identification of proposed remediation actions.

To define the role, the human resource officer developed a job description by combining elements from the ECSF's CISO and Cybersecurity Risk Manager role profiles. Once filled, the was formally designated as CISO in the organisation's organigram.

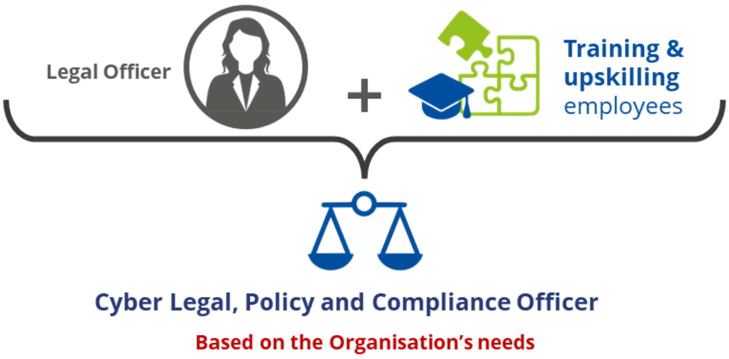
Figure 2: Combination of 2 ECSF role profiles based on the organisational needs


Chief Information Security Officer (CISO)
+
Cybersecurity Risk Manager
Role Profiles Combined and Modified
Cybersecurity Manager
Based on Organisation's needs

Step 2: Upskill the Legal Officer

The Legal Officer, already managing compliance with legal and regulatory frameworks, expressed interest in enhancing her skills in privacy and cybersecurity legal matters to address tasks **5** and **6**. Human Resources department supported her upskilling using a list of key knowledge and skills from the ECSF. She eventually upskilled to a Cyber Legal, Policy and Compliance Officer.

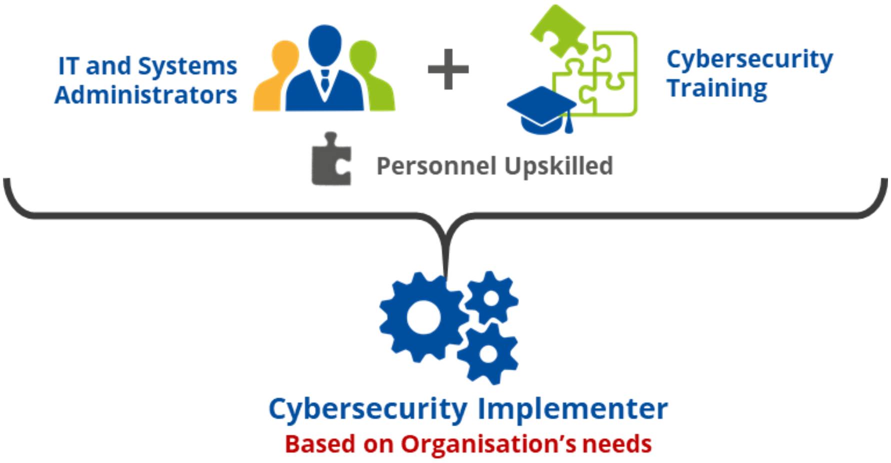
Figure 3: Upskilling the Legal Officer


Legal Officer
+
Training &
upskilling
employees
Cyber Legal, Policy and Compliance Officer
Based on the Organisation's needs

Step 3: Upskill the IT and Systems Administrators and Support the Design and integration of Secure Digital Solutions

The IT and Systems Administrators were following different cybersecurity best practices and frameworks and worked mostly in an ad-hoc way without a strategy or structure. To address task **7**, the CISO decided to upskill the IT and Systems Administrators through targeted training, utilising a list of key knowledge and skills from the ECSF[10]. This enabled them to securely implement, operate, maintain, and support technical solutions, including secure configuration, patch management and system testing. This upskilling also prepared the IT and Systems Administrators to participate effectively in incident response efforts, working in close collaboration with external specialists to address task **10**.

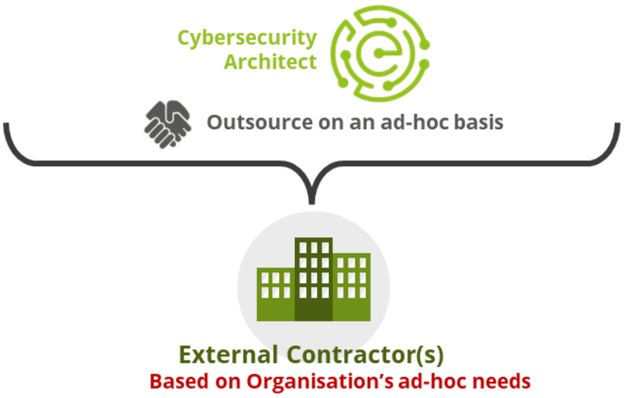
Figure 4: Upskilling IT and System Administrators



The organisation also lacked the internal competencies necessary to design and integrate secure digital solutions. Consequently, the CISO opted to outsource this function on an ad-hoc basis.

Figure 5: Outsourcing on an ad-hoc basis

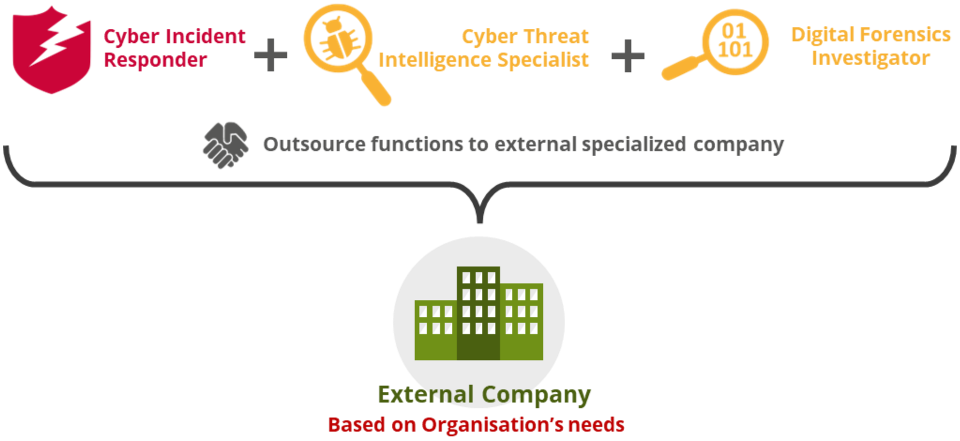
[10] European Cybersecurity Skills Framework (ECSF): https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf


Cybersecurity Architect
Outsource on an ad-hoc basis
External Contractor(s)
Based on Organisation's ad-hoc needs

Step 4: Outsource Cyber Threat Intelligence and Incident Response

To address tasks **9** and **10**, the CISO decided to outsource the Cyber Incident Response, the Cyber Threat Intelligence and the Digital Forensics Investigation responsibilities to a specialised organisation able to provide continuous monitoring, advanced threat detection, digital forensics analysis and effective containment measures, ensuring a rapid and coordinated response. Service Level Agreements (SLAs) were clearly defined to set expectations around response times and quality of service. However, reporting obligations could not be delegated, so the CISO retained responsibility for reporting incidents in accordance with regulatory requirements. Recognising that successful incident response requires collaboration between internal and external teams, the CISO acknowledged the need to upskill internal IT and Systems Administrators- —a need that is addressed in Step **3.**

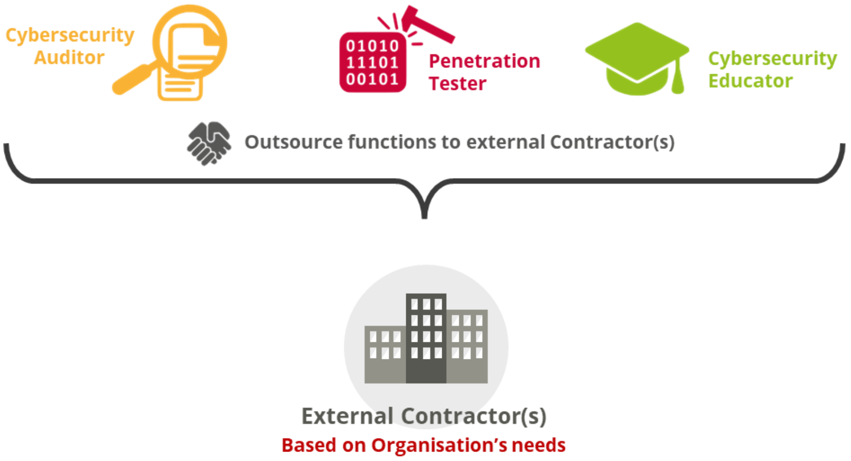
Figure 6: Outsourcing of Cyber Incident Response, the Cyber Threat Intelligence and the Digital Forensics Investigation responsibilities


Cyber Incident Responder
+
Cyber Threat Intelligence Specialist
+
01 101
Digital Forensics Investigator
Outsource functions to external specialized company
External Company
Based on Organisation's needs

Step 5: Engaging External Expertise for Specialised Support

Due to a lack of internal competencies, the CISO decided to outsource the non-recurring tasks **4**, **8** and **11** to external experts, based on a cost-effective analysis and prioritisation of tasks. By leveraging the ECSF, the CISO identified key tasks to be outsourced—namely, **periodic cybersecurity audits, penetration testing and vulnerability assessments, and tailored cybersecurity training**. Specialised providers were contracted to deliver these services, with clear Service Level Agreements (SLAs) in place to define their scope, timelines, and performance standards.

Figure 7: Outsourcing on an ad-hoc basis



Step 6: Continuous Monitoring and Improvement

To ensure continuous improvement and accountability, the CISO, in collaboration with senior management, introduced a monitoring mechanism based on clearly defined Key Performance Indicators (KPIs) and success criteria. These indicators were used to measure the progress and effectiveness of each step-action outlined in the roadmap.

3.1.4 Summary

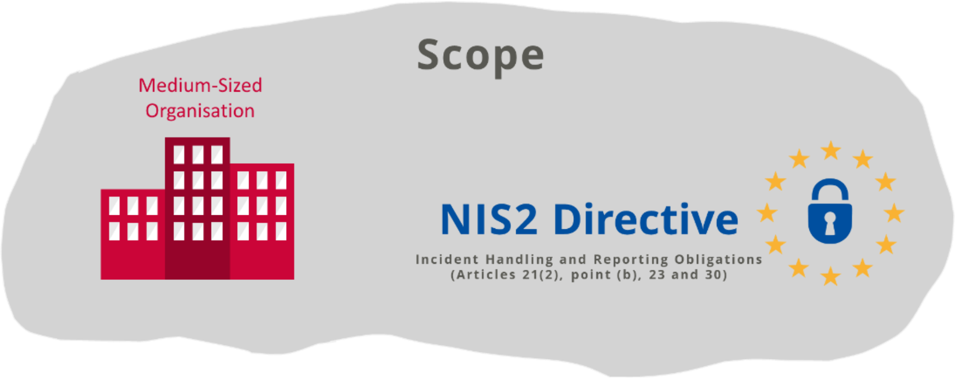
This use case illustrates how a medium-sized organisation can use the ECSF to develop a cybersecurity organisational framework, in order to work towards NIS2 Directive implementation. By providing a comprehensive mapping of required responsibilities and skills, the ECSF enabled the organisation to systematically address its cybersecurity needs. The framework facilitated strategic organisational alignment, guiding the management in hiring a dedicated cybersecurity manager, upskilling existing staff, and outsourcing critical functions like threat intelligence and incident response and occasional tasks like conducting security audits, security scans and training. This structured approach also enhances the organisation's overall cybersecurity posture, demonstrating the ECSF's vital role in fostering robust cybersecurity practices within organisations.

3.2 SCENARIO 2: NIS2 IMPLEMENTATION FOR POST-INCIDENT RESPONSE AND REPORTING

In this example, we focus solely on post-incident response and reporting obligations **(10Task 10),** within the same medium-sized organisation. We will illustrate how the requirements of the NIS2 Directive can be effectively addressed through the tasks and cooperation of ECSF role profiles within the organisation.

TARGETED SCENARIO ADAPTATION
Scenarios can be tailored to specific NIS2 obligations, such as post-incident response and reporting, helping entities address gaps and resource constraints in key areas.

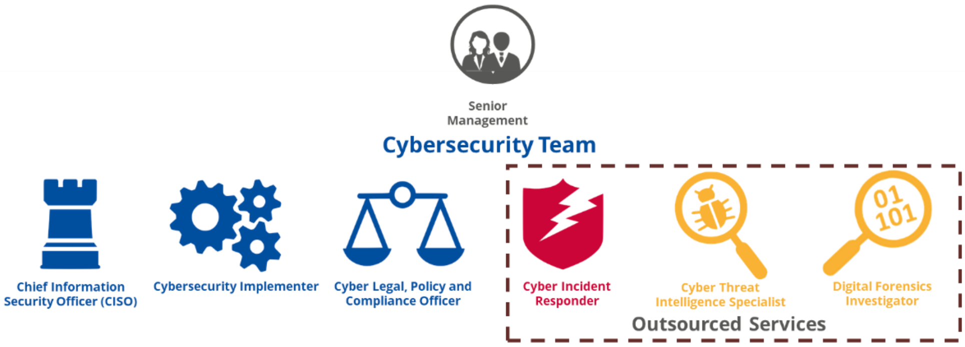
Figure 8: A Medium-Sized Organisation subject to post-incident response and reporting obligations


Scope
Medium-Sized Organisation
NIS2 Directive
Incident Handling and Reporting Obligations (Articles 21(2), point (b), 23 and 30)

3.2.1 The Team

To meet the cyber incident response and reporting requirements, senior management established a team of skilled professionals. Recognising that, as a medium-sized company, they lacked the internal capacity, skills, or resources to fully staff a dedicated internal team, they leveraged three (3) pre-established roles, the CISO, a Cybersecurity Implementer, and the Cyber Legal, Policy and Compliance Officer, alongside the external specialised organisation providing Incident Response, Threat Intelligence, and Digital Forensics services. The team's objective was to ensure effective response and reporting of cybersecurity incidents, fully aligning with NIS2 compliance requirements.

Figure 9: Establishing a cybersecurity team


Senior Management
Cybersecurity Team
Chief Information Security Officer (CISO)
Cybersecurity Implementer
Cyber Legal, Policy and Compliance Officer
Cyber Incident Responder
Cyber Threat Intelligence Specialist
Digital Forensics Investigator
Outsourced Services

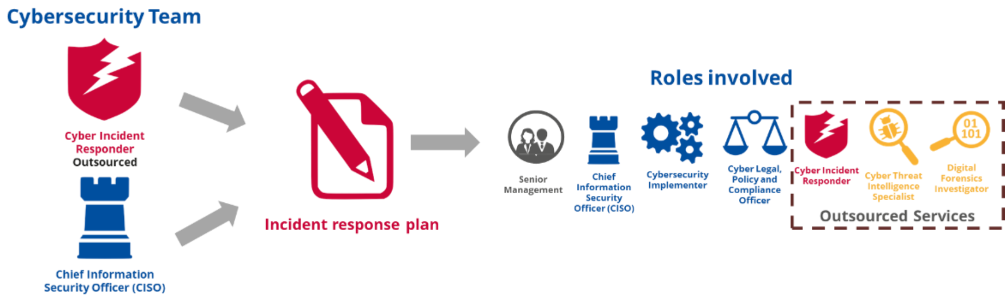
3.2.2 Organisational Alignment and Implementation through Resource Allocation

To effectively address the organisational tasks detailed in the previous section, the senior management implemented the following steps.

Step 1: Develop an Incident Response Plan

The team's first step was to develop an Incident Response Plan. The CISO with support from the outsourced service, drafted the plan. Roles and responsibilities were clearly defined and communicated to the entire team. The incident response plan also included templates for any kind of incident report indicated in Article 23(4).

Figure 10: Incident response plan involvement


Cybersecurity Team
Cyber Incident Responder Outsourced
Chief Information Security Officer (CISO)
Incident response plan
Roles involved
Senior Management
Chief Information Security Officer (CISO)
Cybersecurity Implementer
Cyber Legal, Policy and Compliance Officer
Cyber Incident Responder
Cyber Threat Intelligence Specialist
01 101
Digital Forensics Investigator
Outsourced Services

Step 2: Incident Response Readiness and Drills

Once the plan was in place, the organisation took steps to ensure readiness through regular testing. The CISO, in coordination with the team, organised periodic incident response tabletop exercises to assess the effectiveness of the plan. These exercises helped the team become familiar with their roles, improved reaction times, and identified areas for improvement.

Step 3: Detecting, Analysing and Classifying an Incident

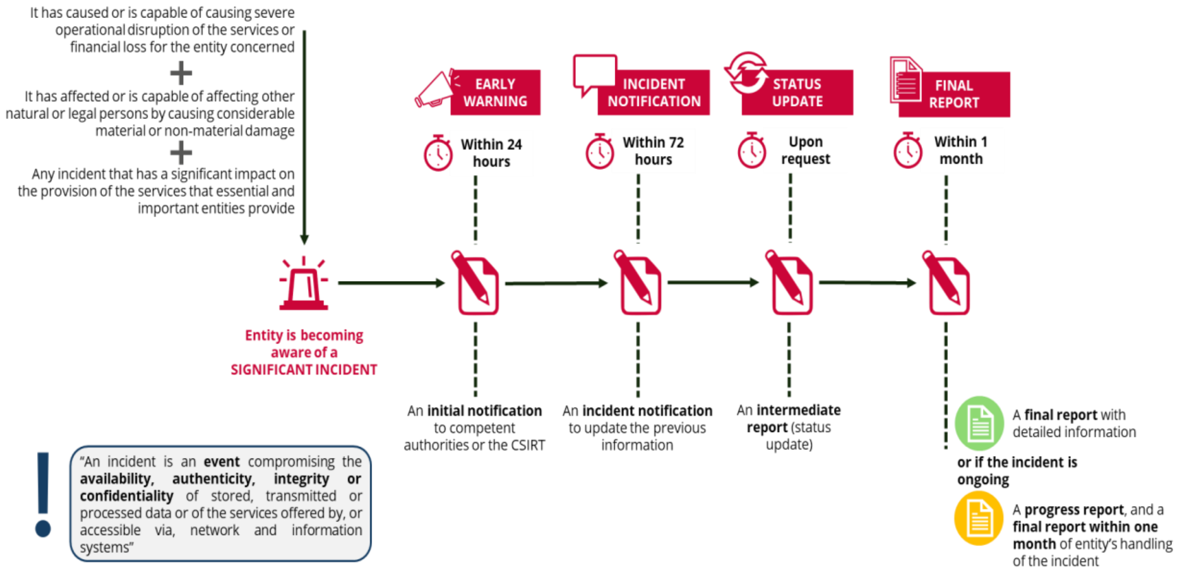
The Cybersecurity Implementer, a Systems Administrator who was upskilled to additionally fulfil this role, received an alert from their network monitoring system indicating a possible sign of a data exfiltration attempt. The Cybersecurity Implementer quickly called the CISO. The CISO collaborated and asked for support from the outsourced service to provide context and the potential impact of the detected activity.

The team began their analysis remotely, identifying a sophisticated phishing attack that had bypassed initial defences and was likely responsible for the suspicious network behaviour. Following the initial analysis, the CISO classified the incident and assessed its severity to determine whether it met NIS2 reporting thresholds. Based on this assessment, the CISO contacted the national CSIRT to request further guidance and support. The CSIRT provided guidance and support on how the team should initially handle the situation. The Cybersecurity Implementer implemented the mitigation measures in accordance with the guidance provided by the CSIRT.

Step 4: Initial Reporting – The 24-hour Window

According to the NIS2 Directive (Article 23(4.a)), the organisation had 24 hours to notify the Computer Security Incident Response Team (CSIRT) and/or the National Competent Authority (NCA) about the incident. After classifying the incident as reportable under NIS2, the CISO, coordinated with the Cyber Legal, Policy and Compliance Officer, to prepare the initial early warning report and also briefed the senior management about the incident. The report was drafted according to the technical details, initial analysis and mitigation measures provided by the Cybersecurity Implementer, and the outsourced services. The report was sent to the CSIRT and/or NCA within the required timeframe using secure communication channels. The overall timeline is presented in the following figure.

Figure 11: Incident notification timeline and actions (as per Article 23(4) of the NIS2D)


It has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned
+
It has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage
+
Any incident that has a significant impact on the provision of the services that essential and important entities provide
EARLY WARNING
Within 24 hours
INCIDENT NOTIFICATION
Within 72 hours
STATUS UPDATE
Upon request
FINAL REPORT
Within 1 month
Entity is becoming aware of a SIGNIFICANT INCIDENT
An initial notification to competent authorities or the CSIRT
An incident notification to update the previous information
An intermediate report (status update)
A final report with detailed information
or if the incident is ongoing
A progress report, and a final report within one month of entity's handling of the incident
!
"An incident is an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems"

Step 5: 72-hour Detailed Report

Over the next 72 hours, the organisation must provide an incident notification report containing the status of the early warning report (where applicable) of **step 3**, an initial assessment of the severity and impact along with indicators of compromise. The CISO, the Cybersecurity Implementer and the outsourced services worked closely, to uncover the full extent of the breach. They identified the entry point, assessed the data that were accessed, and recommended immediate actions to contain the threat.

The CISO and the Cyber Legal, Policy and Compliance Officer collaborated to compile the detailed report based on the outsourced services input. The report included the severity and impact on the organisation's services and indicators of compromise (i.e., unusual network traffic and unauthorised user activity). The comprehensive report was submitted to the CSIRT and/or NCA within the 72-hour deadline.

Step 6: Continuous Communication and Intermediate Reports

After the 72-hour incident notification report, the team, upon the request of the CSIRT and/or the NCA, must provide an intermediate report on relevant status updates with their severity and impact. The CISO, the Cybersecurity Implementer and the outsourced services worked together to mitigate and contain the incident, gathered additional evidence, and sought support from the CSIRT for further containment efforts.

Throughout the process, the CISO maintained open lines of communication with the CSIRT and/or NCA, providing updates on the mitigation efforts. The CISO also collaborated with the Cyber Legal, Policy and Compliance Officer to compile an intermediate report on the status of the incident based on the Cybersecurity Implementer and the outsourced services input after the request of the CSIRT. This collaborative effort was essential in ensuring the organisation's response met regulatory expectations.

Step 7: Final Report

Within one month of submitting the incident notification report, the organisation must provide a final report[11]. This report must contain a comprehensive description of the incident, including the

[11] in the event of an ongoing incident at the time of the submission of the final report, the entities concerned must provide a progress report at that time and a final report within one month of their handling of the incident.

type of threat or root cause, implemented and ongoing mitigation measures, and, if applicable, the cross-border impact of the incident.

The CISO, the Cybersecurity Implementer and the outsourced services continued their efforts and successfully contained the incident. They also collected additional evidence to be included in the final report.

The CISO and the Cyber Legal, Policy and Compliance Officer collaborated with the team and prepared the final report based on the Cybersecurity Implementer's report on the mitigation measures and input from the outsourced services. Throughout each step, the CISO engaged the senior management and informed them about the incident status, actions taken, required resources, and implemented mitigation measures.

Step 8: Post-Incident Review and Follow-Up

In the last step, the team convened for a post-incident review to conduct a Lessons Identified/Lessons Learned (LI/LL) exercise and assess the effectiveness of measures taken to prevent future incidents. Based on this analysis, they agreed to strengthen the organisation's cybersecurity posture through the following actions:

Team members	Actions
Chief Information Security Officer (CISO)	Strengthen coordination with third-party forensic and threat intelligence teams by establishing formal communication protocols and developing a unified incident response playbook. Improve real-time monitoring capabilities by deploying advanced threat detection tools and refining alert thresholds based on recent incident patterns.
Cyber Legal, Policy and Compliance Officer	Revise incident reporting procedures to reduce response times and ensure more precise compliance with regulatory requirements. Develop a legal risk assessment framework to proactively address changes in regulations and improve legal response preparedness.
Cybersecurity Implementer	Implement improvements based on lessons learned, ensuring that all mitigation measures are applied effectively. Collaborate with the CISO to refine security controls and enhance the resilience of critical systems. Support the Incident Response service by integrating findings into updated response strategies.
Incident Response Service (outsourced)	Develop an incident playbook with lessons learned to standardise response actions and improve efficiency. Design and conduct targeted training and simulation exercises (with the help of a Cybersecurity Educator) based on the incident's unique challenges to enhance the team's readiness.
Cyber Threat Intelligence Service (outsourced)	Refine the threat intelligence strategy by focusing on newly identified vulnerabilities and emerging threats relevant to the organisation.

Team members	Actions
Digital Forensics Service (outsourced)	Establish a more integrated role in the incident response process by participating in regular drills and sharing forensic best practices. Create a standardised evidence collection protocol to ensure consistency and legal integrity across all investigations.

3.2.3 Summary

In conclusion, this example illustrates how the medium-sized organisation can effectively address the post-incident response and reporting obligations outlined in **10Task 10** (Article 23, NIS2 Directive). By establishing a dedicated team with clearly defined roles and responsibilities, including both internal and external resources, the organisation implements the NIS2 requirements. This step-by-step approach demonstrates how specific tasks and collaborations between ECSF role profiles can be leveraged to manage incidents efficiently, meet reporting deadlines, and minimise impact. This structured and collaborative method not only aligns with regulatory expectations but also strengthens the organisation’s cybersecurity posture and resilience against future incidents.

4. DETAILED MAPPING OF ECSF AND NIS2

This section provides a detailed table outlining, for each ECSF role profile, the main NIS2 responsibilities, obligations, deliverables, and potential collaborations with other ECSF role profiles, organised by relevant NIS2 articles.

#	Role Profile		NIS2 Main Responsibility	NIS2 Obligations (tasks)	Deliverables (non-exhaustive list)
1	♜	**Chief Information Security Officer (CISO)**	Manages an essential or important entity's cybersecurity strategy and its implementation to align with the Directive's requirements (Articles 20 and 21)	- Exchanges information and provides reports to competent authorities and other interested parties (Articles 3(4), 27(2,3), 32(4.b,4.c, 4.d, 4.e, 4.f, 5) and 33(4.b,4.c, 4.d, 4.e, 4.f) - Presents cybersecurity plans and strategies to the management board (Articles 20(1) and 21(2)) - Educates members of the management bodies about cybersecurity risks, threats and their impact on the entity (Article 20.2) - Defines strategy and policies to align with the Directive (Article 21(2.a)) - Creates processes for business continuity plan (BCP) and disaster recovery plan (DRP), (Article 21(2.c)) - Analyse and implement policies and procedures on risk analysis, information system security, supplier management security, encryption, role-based access, asset management, human resources and others (Articles 21(2.a, 2.d, 2.h, 2.i) and 28(3)) - Manages relationships with suppliers and service providers to ensure supply chain security (Article 21(2.d)) - Presents the cybersecurity risk-management measures to the members of the management bodies (Article 20(1)) - Manages the implementation of binding instructions or orders (Articles 32(4.b, 4.f, 5) and 33(4.b, 4.f) - Manages the cybersecurity policy of the entity and assigns responsibilities to other roles in order to implement the measures and fulfil the reporting obligations (Articles 32(4.c, 4.d) and 33(4.c, 4.d)	- Cybersecurity policies and procedures (Article 21(2)) - Business Continuity Plan (Article 21(2.c)) - Disaster Recovery Plan (Article 21(2.c)) - Suppliers Security Policy (Article 21(2.d)) - Encryption Policy (Article 21(2.h)) - Incident Response Plan (Articles 21(2.b) and 23) (In cooperation with the Cyber Incident Responder) - Cyber Incident Report (Articles 21(2.b), 23(4) and 30(1)) (Including early warning, voluntary notifications, progress and post-incident analysis reports in cooperation with the Cyber Incident Responder and the Cyber Legal, Policy and Compliance Officer) - Compliance Manual (Articles 1, 2, 3, 4, 20, 26, 27, 28 and 29) (Contains all regulatory compliance obligations. Created in cooperation with the Cyber Legal, Policy and Compliance Officer, regular reviews and updates must be in place to stay current with evolving regulations) - Cybersecurity Requirements Report (Article 21) (In cooperation with the Cybersecurity Architect) - Secure System Acquisition and Development Policy (Article 21(2.e)) (In cooperation with the Cybersecurity Architect) - Internal Audit Policy and Procedure (Article 21(2.a, 2.f)) (In cooperation with the Cybersecurity Auditor) - Cybersecurity Awareness Programme (Articles 20(2) and 21(2.g)) (Aimed at members of management bodies of entities and their employees in cooperation with the Cybersecurity Educator) - Cybersecurity Training Material (Articles 20.2 and 21(2.g)) (In cooperation with the Cybersecurity Educator) - Deployment and Operation Procedure (Article 21.2) (In cooperation with the Cybersecurity Implementer) - Implementation Report (Articles 21(2), 32(4, 5) and 33(4)) (After the security audits of articles 32 and 33 or the risk assessment, the internal or external audit, the vulnerability scans and/or penetration tests, and the management review meetings in cooperation with Cybersecurity Implementer)

#	Role Profile		NIS2 Main Responsibility	NIS2 Obligations (tasks)	Deliverables (non-exhaustive list)
					- Internal Audit Policy and Procedure (Article 21(2.a, 2.f)) (In cooperation with the Cybersecurity Auditor)
2		**Cyber Incident Responder**	Ensures an effective response to cybersecurity incidents and comprehensive reporting of these incidents (Articles 21 and 23)	- Cooperates with competent authorities and participates in national large-scale cybersecurity incident and crisis response plans and exercises (Article 9(4)) - Set up an incident response plan (Article 9(4)) - Cooperates and exchanges information with CSIRTs (Articles 10(4) and 11(4)) - Requests real-time or near real-time monitoring from the CSIRTs to monitor and assess the cybersecurity state of the entity's network and system (Article 11(3.a)) - Requests and receives assistance from CSIRTs to respond to cyber incidents (Article 11(3.c)) - Requests proactive scanning of the network and information systems from the CSIRTs to monitor and assess the cybersecurity state of the entity's network and system (Article 11(3.e)) - Evaluates and reports any vulnerabilities to the CSIRT (Article 12). - Handles cybersecurity incidents and discloses vulnerabilities (Article 21(2.b, 2.e)) - Identifies, analyses and reports cybersecurity incidents to the CSIRTs or the competent authorities and the recipients of the services provided by the entity (Article 23(1)) - Prepares, cooperates with, and provides input for submitting early warning reports, progress reports and final cyber incident reports to the CSIRTs or the competent authorities in a specific manner and time (Article 23(4)) - Provides information to CSIRTs or competent authorities in the form of voluntary notifications about cybersecurity incidents and near misses (Article 30(1)) (voluntary)	- Incident Response Plan (Articles 21(2.b, 2.e) and 23) (In cooperation with the CISO) - Cyber Incident Report (Articles 21(2.b), 23(4) and 30(1)) (Including early warning, voluntary notifications, progress and post-incident analysis reports in cooperation with the CISO, the Digital Forensics Investigator and the Cyber Threat Intelligence Specialist)
3		**Cyber Legal, Policy and Compliance Officer**	Oversees and assures compliance with the Directive (Articles 1, 2, 3, 4, 20, 26, 27, 28 and 29)	- Oversees and assures compliance with the Directive by ensuring the adoption of cybersecurity risk-management measures, the reporting of cybersecurity incidents and the information sharing with other entities, competent authorities and CSIRTs (Articles 1(2.b, 2.c), 3(4) and 4(1, 2)) - Oversees and assures compliance with the Directive if the entity falls within its scope and processes personal data to the extent necessary for this Directive and in accordance with Regulation (EU) 2016/679 (Article 2(1, 2, 3, 4, 5, 7, 8, 9, 10, 14)) - Informs the management bodies of essential and important entities that they can be held liable for infringements if their entities won't approve the cybersecurity risk-management measures taken by their	- Compliance Manual (Articles 1, 2, 3, 4, 20, 26, 27, 28 and 29) (Contains all regulatory compliance obligations. Created in cooperation with the CISO) - Compliance Report (Articles 1, 2, 3, 4, 20, 26, 27, 28 and 29) (e.g., Gap Analysis, which includes all articles referring to essential and important entities' liabilities) - Data Protection Impact Assessment or Privacy Impact Assessment (Articles 2 and 28(1, 2, 5)) - Cyber Incident Report (Articles 21(2.b), 23(4) and 30(1)) (Including early warning, voluntary notifications, progress and post-incident analysis reports in cooperation with the CISO)

#	Role Profile		NIS2 Main Responsibility	NIS2 Obligations (tasks)	Deliverables (non-exhaustive list)
				entities in order to comply with Article 21 and that they are required to follow cybersecurity training (Article 20) - Oversees and assures compliance with the Directive by informing the senior management of the entity that must designate a representative if the entity is not established in the EU but offers its services in the EU (Article 26(3, 4)) - Oversees and assures compliance with the Directive by ensuring the submission of information to the competent authorities to register in the national list of essential and important entities and notify them about any changes (Article 27(2, 3)) - Oversees and assures compliance with the Directive by ensuring the proper collection, processing, verification and access provision of domain name registration data by Top Level Domain (TLD) name registries and entities providing domain name registration services (Article 28) - Oversees and assures compliance with the Directive by ensuring that their entities are notifying the competent authorities of their participation in the cybersecurity information-sharing arrangements referred to in Article 29(2), upon entering into such arrangements, or, as applicable, of their withdrawal from such arrangements, once the withdrawal takes effect (Article 29(4))	
4		Cyber Threat Intelligence Specialist	Collects, processes and analyses data and information to identify significant cyber threats (Articles 21, 23, 29 and 30)	- Identifies significant cyber threats by collecting, analysing and producing cyber threat reports and communicates these reports and any measures or remedies that must be taken to the recipients of their services (Article 23(2)) - Manages the cyber threat intelligence life cycle, including collection, analysis, production, and exchange of cybersecurity information between the community essential and important entities and their suppliers and service providers, including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding the configuration of cybersecurity tools to detect cyberattacks (Article 29(1, 2)) (voluntary) - Provides information to CSIRTs or competent authorities in the form of voluntary notifications about cyber threats (Article 30(1)) (voluntary)	- Cyber Threat Intelligence Manual (Articles 23(2), 29(1, 2) and 30(1)) - Cyber Threat Report (Article 23(2)) - Cyber Incident Report (Articles 21(2.b), 23(4) and 30(1)) (Including early warning, voluntary notifications, progress and post-incident analysis reports that include cyber threats in cooperation with the Cyber Incident Responder and the Digital Forensics Investigator)
5		Cybersecurity Architect	Plans and designs security-by-design solutions to align with the	- Plans and designs secure networks and establishes a secure environment during the development lifecycle (Article 21(2.e)) - Develops and implements robust security measures, such as multi-factor authentication (MFA), secured	- Cybersecurity Architecture Diagram (Article 21(2.e)) - Cybersecurity Requirements Report (Article 21) (Analyses and evaluates the cybersecurity of the entity's architecture in order to align with the cybersecurity risk measures of the Directive and provides the Cybersecurity Requirements

#	Role Profile		NIS2 Main Responsibility	NIS2 Obligations (tasks)	Deliverables (non-exhaustive list)
			cybersecurity risk measures of the Directive (Article 21)	voice, video, and text communications, and secured emergency communication systems (Article 21(2.j)) - Designs secure architectures and utilises qualified trust services and certified ICT products, ICT services and ICT processes under the Cybersecurity Act (Article 24(1))	Report to be presented to the management bodies in cooperation with the CISO) - Secure System Acquisition and Development Policy (Article 21(2.e)) (In cooperation with the CISO)
6		Cybersecurity Auditor	Performs cybersecurity audits to assess alignment with the Directive and uncover areas for enhancement. (Articles 20, 21, 23 and 32)	- Conducts audits to assess the implementation of cybersecurity training for management bodies and employees, risk management measures, and reporting obligations under the Directive. (Articles 20, 21 and 23) - Conducts internal security audits, compiles and provides, when requested, the internal audit reports to the competent authorities (Article 32(2.e, 2.g))	- Cybersecurity Audit Plan (Articles 20, 21, 23 and 32) - Cybersecurity Audit Report (Articles 20, 21, 23 and 32) - Internal Audit Policy and Procedure (Article 21(2.a, 2.f)) (In cooperation with the CISO)
7		Cybersecurity Educator	Creates and delivers cybersecurity awareness and training programmes for members of management bodies and employees to enhance their understanding and competencies in line with the Directive's requirements (Articles 20 and 21)	- Creates and delivers appropriate cybersecurity training programmes aimed at members of management bodies of entities and their employees (Article 20(2)) - Implements basic cyber hygiene practices and designs and delivers cybersecurity training (Article 21(2.g))	- Cybersecurity Awareness Programme (Articles 20(2) and 21(2.g)) (Aimed at members of management bodies of entities and their employees. In cooperation with the CISO) - Cybersecurity Training Material (Articles 20(2) and 21(2.g)) (In cooperation with the CISO) - Training Effectiveness Reports (Articles 20(2) and 21(2.g))
8		Cybersecurity Implementer	Implements cybersecurity solutions and controls based on the cybersecurity risk-management measures of the Directive (Articles 21, 32 and 33)	- Develops, deploys, operates and monitors cybersecurity solutions such as secure network configuration and secure integration and configuration of information systems (Article 21(2.e)) - Implements cybersecurity solutions, within the time limit specified, to mitigate the findings of a security audit (Articles 32(4, 5) and 33(4))	- Cybersecurity Solutions (Documentation of objectives, scope, requirements, detailed design specifications, implementation plan, configuration settings, integration points, maintenance, testing, etc.) (Article 21(2)). - Deployment and Operation Procedure (Article 21(2)) (In cooperation with the CISO) - Implementation Report (Articles 21(2), 32(4, 5) and 33(4)) (After the security audits of articles 32 and 33 or the risk assessment, the internal or external audit, the vulnerability scans and/or penetration tests, and the management review meetings in cooperation with the CISO)
9		Cybersecurity Researcher	Researches the cybersecurity domain and incorporates results in cybersecurity solutions based on the cybersecurity risk-management measures of the Directive (Article 21)	- Conducts research to advance cybersecurity technologies, solutions, developments and processes (Article 21(2)) - Recommends advanced cybersecurity solutions based on research (Article 21(2)) - Develops proof of concept, pilots and prototypes for cybersecurity solutions (Article 21(2))	- Research and Development Reports (Makes recommendations through research reports for more secure solutions, e.g., research on encryption to protect from post-quantum threats) (Article 21(2)) - Proof of Concept and Prototype Documentation (Article 21(2))
10		Cybersecurity Risk Manager	Manages the entity's cybersecurity-related risks aligned to its strategy	- Creates risk assessment reports and risk remediation action plans to assess and improve the effectiveness of cybersecurity risk-management measures and provide	- Cybersecurity Risk Assessment Report (Articles 21(2.f), 21(3), 32(2.b) and 33(2.b)) - Cybersecurity Risk Remediation Action Plan (Articles 21(2.f), 21(3), 32(2.b) and 33(2.b))

#	Role Profile		NIS2 Main Responsibility	NIS2 Obligations (tasks)	Deliverables (non-exhaustive list)
			and the Directive’s requirements (Article 21)	these reports to the competent authorities (Articles 21(2.f), 32(2.b) and 33(2.b)) - Assesses suppliers' security and takes into account the results of the coordinated security risk assessments of critical supply chains (Article 21(3))	
11		Digital Forensics Investigator	Investigates cybersecurity incidents and presents digital evidence to support the entity in meeting the reporting obligations of the Directive (Article 23)	- Contributes to early warnings, updates and final reports of cybersecurity incidents by providing analysis, reconstruction and interpretation of the digital evidence based on a qualitative opinion (Article 23(4))	- Digital Forensics Analysis Results (Article 23(4)) - Electronic Evidence (Article 23(4)) - Cyber Incident Report (Article 23(4)) (Including early warning, voluntary notifications, progress and post-incident analysis reports in cooperation with the Cyber Incident Responder and the Cyber Threat Intelligence Specialist)
12		Penetration Tester	Conduct penetration testing to assess the effectiveness of cybersecurity solutions against the cybersecurity risk management measures of the Directive (Articles 21, 32 and 33)	- Conducts penetration tests and vulnerability assessments in order to assess the effectiveness of cybersecurity solutions and provides, when requested, the vulnerability assessment and/or penetration testing reports to the competent authorities (Articles 21(2), 32(2.d, 3) and 33(2.d, 3)) - Assists the competent authorities' personnel on the security scans conducted (Article 32(2.d, 3) and 33(2.d, 3))	- Vulnerability Assessment Results Report (Articles 21(2), 32(2.d, 3) and 33(2.d, 3)) - Penetration Testing Report (Articles 21(2), 32(2.d, 3) and 33(2.d, 3))

4.1 MAPPING BENEFITS

A few benefits of mapping ECSF role profiles to the NIS2 Directive include the following.

- **Enhanced accountability and governance.** By clarifying key roles and tasks, this mapping enables senior management to more effectively oversee cybersecurity compliance efforts, improving governance and ensuring that leadership is fully aware of their responsibilities under NIS2.
- **Optimised organisational structure.** It helps develop a clear structure by defining which tasks can be outsourced and streamlining cybersecurity operations, improving overall efficiency in managing cyber risks.
- **Clear role definitions for meeting NIS2 requirements.** The mapping provides precise role descriptions aligned with NIS2 obligations, ensuring that each team member understands their specific duties, reducing confusion and enhancing accountability.
- **Streamlined incident response and reporting.** It promotes a structured approach to incident management, enabling faster, more efficient handling of security events and ensuring timely, compliant reporting.
- **Task alignment with NIS2 requirements.** Roles and tasks are tailored to meet NIS2 obligations, minimising ambiguity.
- **Targeted workforce development.** By using certifications already aligned with the ECSF[12], organisations can better advance the workforce skillset to meet NIS2 requirements.
- **Role-based implementation of NIS2 for Member States.** Mapping NIS2 obligations to ECSF roles helps national authorities translate legal and policy texts into practical, role-based responsibilities. This makes it easier to develop actionable national guidance and bridge the gap between legislation and execution.
- **Strategic workforce planning and capacity building.** By identifying the specific roles and skills needed to meet NIS2 obligations, national authorities can better allocate resources toward national training programmes, upskilling initiatives, and curriculum development. This supports long-term national workforce planning and capacity building.
- **Enhancing national cybersecurity maturity.** National authorities can use the mapping to assess the maturity of the national cybersecurity workforce, identify gaps in critical roles (e.g., incident response, supply chain security) and build strategies to close them through incentives, reforms or public–private partnerships.

Organisations can strengthen their cyber resilience by aligning ECSF roles with NIS2

Member States can support implementation, close skills gaps, and build long-term cyber capacity

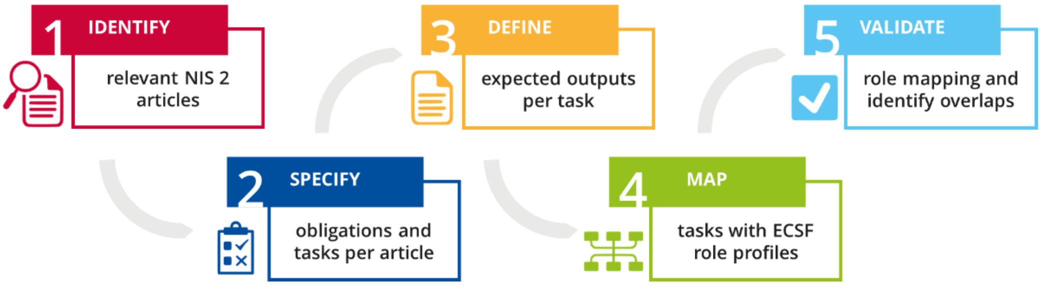
The ECSF role profile mapping is more than just a tool for organisations working toward NIS2 compliance and stronger cybersecurity practices — it's also a valuable resource for Member States. By using the mapping methodology outlined in this guide, and illustrated through practical use cases, policymakers and national competent authorities can make more informed decisions when planning workforce development, shaping sector-specific implementation roadmaps, and strengthening national incident response capabilities. In this way, the ECSF role profile mapping serves not only as an organisational asset but also as a strategic enabler for Member States as they work to build long-term cybersecurity capacity.

[12] Certifications mapped to the ECSF: https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf/certifications-mapped-to-the-ecsf.

ANNEX I: METHODOLOGY

This annex explains the approach taken to align the obligations outlined in the NIS2 Directive with the relevant role profiles from the ECSF. The process was carried out in a structured manner, ensuring that each step logically built on the previous one to create a clear, practical, and actionable mapping.

Figure 12: Methodological steps


1 IDENTIFY
relevant NIS 2 articles
2 SPECIFY
obligations and tasks per article
3 DEFINE
expected outputs per task
4 MAP
tasks with ECSF role profiles
5 VALIDATE
role mapping and identify overlaps

STEP 1: IDENTIFY RELEVANT NIS2 ARTICLES

The first step was to identify the specific articles of the NIS2 Directive that outline the obligations for essential and important entities. To achieve this, we conducted a thorough review of each article, isolating only those provisions that directly pertain to these entities. References to other stakeholders, such as the European Commission, Member States' Competent Authorities, ENISA and CSIRTs, were deliberately excluded from this analysis.

STEP 2: SPECIFY OBLIGATIONS AND TASKS PER ARTICLE

In this step, we identified and extracted specific cybersecurity-related obligations from each article, paragraph and point of the NIS2 Directive. These obligations include tasks related to cybersecurity risk management measures, supervision, reporting, and communication.

For instance, Article 32(4)(f) states: *"order the entities concerned to implement the recommendations provided as a result of a security audit within a reasonable deadline."* Based on this, the corresponding task was defined as: *"Implements cybersecurity solutions, within the time limit specified, to mitigate the findings of a security audit."*

This approach ensures that each obligation is clearly formulated as an actionable task, making it easier for entities to understand and implement NIS2 requirements.

STEP 3: DEFINE EXPECTED OUTPUTS PER TASK

In step 3, we defined the expected outputs or deliverables for each cybersecurity-related task identified in the previous phase. These outputs serve as concrete evidence of task completion. Clearly defining deliverables ensures that entities have measurable goals, can track progress, demonstrate accountability, and provide documentation for audits or supervisory reviews. For example, the task *"Implements cybersecurity solutions, within the time limit specified, to mitigate the findings of a security audit"* results in the deliverable *"Implementation Report"*.

STEP 4: MAP TASKS WITH ECSF ROLE PROFILES

In this step, we mapped each cybersecurity-related task identified in the previous phase to the relevant ECSF role profiles. This mapping was guided by the summary statements, mission tasks, main tasks, deliverables, key skills, key knowledge, and e-competences associated with each role.

To establish these connections, we identified relevant keywords and similar tasks. These elements helped align each NIS2 task with the appropriate ECSF role profiles, ensuring a structured and competency-driven approach.

Initially, this mapping was conducted broadly to capture all potential role associations. This approach ensured that no relevant role profiles were overlooked before refining the task-to-role connections in subsequent steps.

STEP 5: VALIDATE ROLE MAPPING AND IDENTIFY OVERLAPS

In the final step, we conducted a critical evaluation of each task-to-role association to enhance the accuracy and reliability of the mapping. This process involved a detailed review by cybersecurity experts to ensure that the selected ECSF skills and knowledge aligned with the practical execution of each task, rather than being influenced by predefined role assumptions.

Given the multidisciplinary nature of cybersecurity, we also identified task overlaps across multiple ECSF role profiles. For instance, while Article 23 primarily focuses on incident handling and reporting, its related tasks require expertise beyond the Cyber Incident Responder role. Instead of restricting the mapping to this profile alone, we carefully examined the full range of ECSF competencies that could realistically contribute to fulfilling these obligations. This methodology prevented role bias and ensured a comprehensive representation.

Finally, we considered how collaboration between different ECSF role profiles may be necessary to deliver the outputs defined in **Step 3**. Many of the expected deliverables — such as cyber incident reports or implementation plans — require input or joint effort from multiple roles. By identifying where such collaboration is essential, the mapping can help entities structure their teams more effectively, allocate responsibilities clearly, and foster inter-role cooperation in meeting NIS2 obligations.

TP-01-25-014-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union’s agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union’s infrastructure, and, ultimately, to keep Europe’s society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

ISBN 978-92-9204-706-1
doi: 10.2824/8870995