enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

NIS2 IMPLEMENTATION
BUILDING YOUR CYBER DEFENCES

Dimitra LIVERI,
Team Leader for Awareness Raising and Education
ENISA

26 | 09 | 2024

IS YOUR SME NOW SUBJECT TO THE NIS2 DIRECTIVE? NOW WHAT?

NIS2

Directive on **measures for a high common level of cybersecurity** across the Union.

MEDIUM-SIZED ORGANISATION

We have to comply with **NIS2**! Where should we start?

EUROPEAN **CYBERSECURITY SKILLS** FRAMEWORK

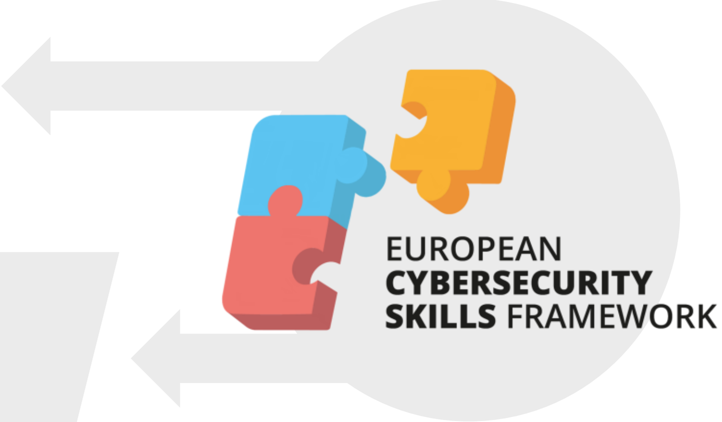
The ECSF can help you!

STEPS TO PREPARE FOR NIS2 COMPLIANCE

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

2 **Strategic Organisational Alignment**
Access 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



The ECSF can assist in completing steps 2 and 3!

IDENTIFYING NIS2 REQUIREMENTS

- □ **Define and implement a cybersecurity plan and policies**
- □ **Conduct risk management, including risk assessment and remediation**
- □ **Collaborate with authorities and other stakeholders**
- □ **Ensure compliance through Cybersecurity Audits**
- □ **Ensure compliance through Cybersecurity Audits**
- □ **Inform stakeholders regarding compliance obligations**
- □ **Plan, design, and implement security solutions and controls**
- □ **Deliver cybersecurity training**
- □ **Collect and analyse information to identify threats**
- □ **Ensure effective response and reporting of cybersecurity incidents**

12 CYBERSECURITY PROFILES

Chief Information Security Officer (CISO)

Cyber Incident Responder

Cyber Legal, Policy and Compliance Officer

Cyber Threat Intelligence Specialist

Cybersecurity Architect

Cybersecurity Auditor

Cybersecurity Educator

Cybersecurity Implementer

Cybersecurity Researcher

Cybersecurity Risk Manager

Digital Forensics Investigator

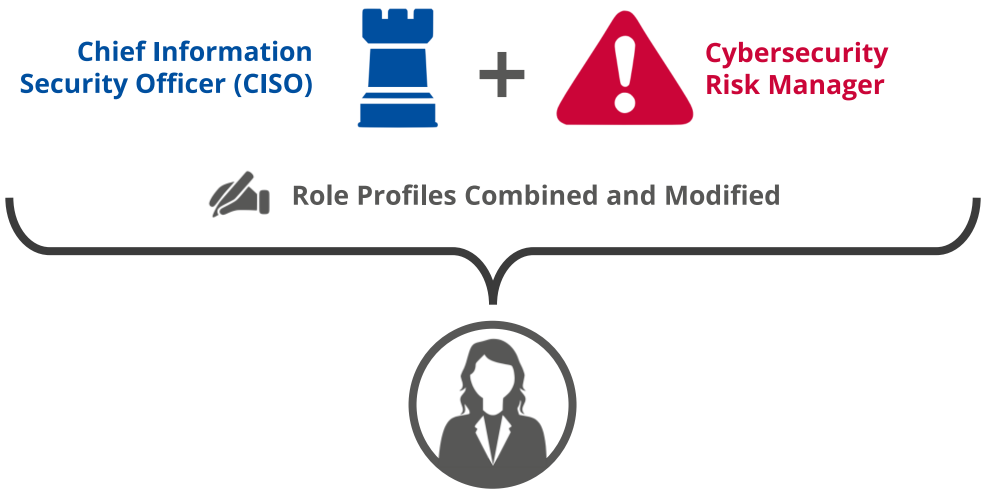
Penetration Tester

EXAMPLE

NEW ROLE REQUIRED

REQUIREMENTS STEMMING FROM NIS2

Assuming that the current personnel can not fulfil the following requirements, we will need to **hire an expert**.



Chief Information Security Officer (CISO) + Cybersecurity Risk Manager

Role Profiles Combined and Modified

Chief Information Security and Risk Officer

Based on Organisation's needs

Using ECSF we can draft the needed position and hire the appropriate expert.

✓ Define and implement a cybersecurity plan 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.

✓ Conduct risk management, including risk assessment and remediation

- 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 company.
- Inform management about cybersecurity risk management measures.

✓ Collaborate with authorities and other stakeholders

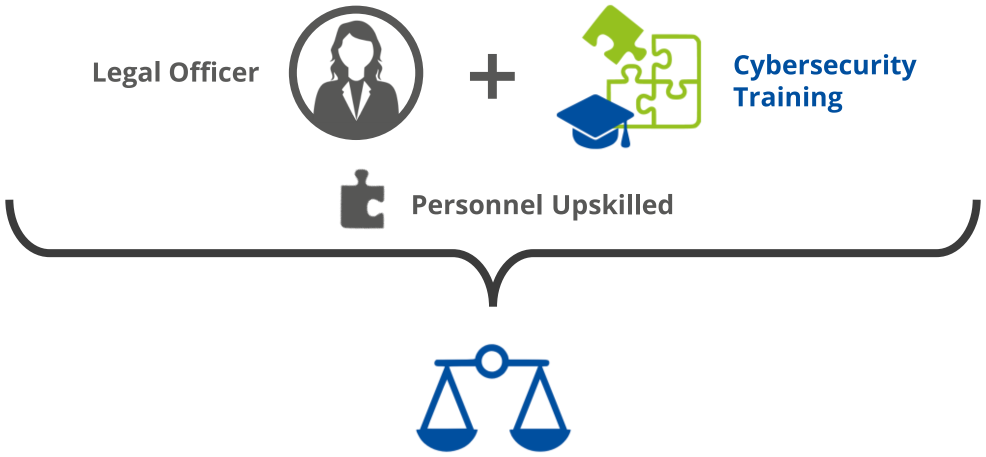
- Share information and provide reports to authorities and other interested parties.
- Ensure compliance with binding instructions or orders from authorities.

EXAMPLE

UPSKILL EXISTING PERSONNEL

REQUIREMENTS STEMMING FROM NIS2

Assuming that our current personnel can fulfil parts of the following requirements, they can be **upskilled through training** to cover them all.



Legal Officer + Cybersecurity Training

Personnel Upskilled

Cyber Legal, Policy and Compliance Officer

Based on Organisation’s needs

Using ECSF we can select the appropriate training to upskill our personnel.

✓ Oversee and assure compliance with the Directive

- Make sure the company 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.

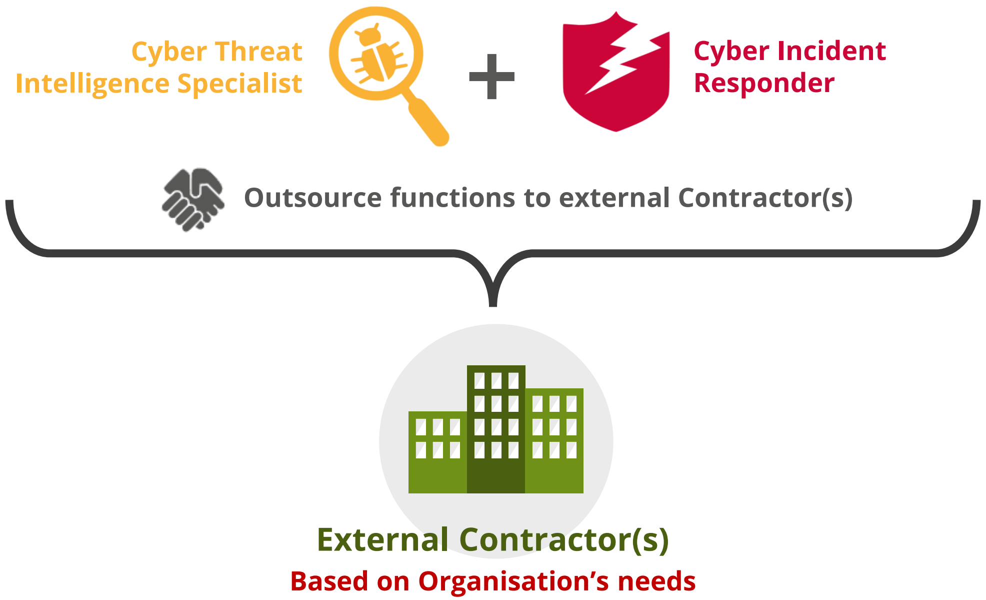
✓ Inform stakeholders regarding compliance obligations

- 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.

EXAMPLE

OUTSOURCING FUNCTIONS

Some **functions can be outsourced** to external contractor(s) with particular expertise.


Cyber Threat Intelligence Specialist
+
Cyber Incident Responder
Outsource functions to external Contractor(s)
External Contractor(s)
Based on Organisation’s needs

Using ECSF we can draft the needed tasks outsource them to the appropriate experts.

✓ Collect and analyse information to identify threats

- Collect and analyze cyber threats, then create reports and share them with relevant parties.
- Oversee the process of collecting, analyzing, and sharing cybersecurity information, including threats, near misses, vulnerabilities, and attack techniques.

✓ Ensure effective response and reporting of cybersecurity incidents

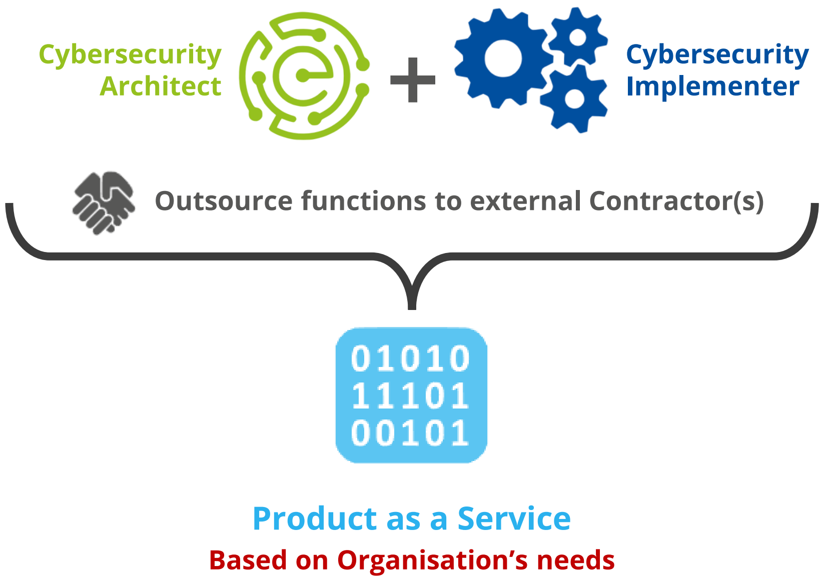
- Develop and establish a plan for responding to cybersecurity incidents.
- Evaluate and report any vulnerabilities to the Computer Security Incident Response Team (CSIRT).
- Manage cybersecurity incidents and disclose any vulnerabilities found.
- Identify, analyze, and report cybersecurity incidents to CSIRTs, authorities, and service recipients.
- Create plans to ensure the business can continue operating and recover quickly in case of a disaster.

EXAMPLE

OUTSOURCING FUNCTIONS

REQUIREMENTS STEMMING FROM NIS2

Some **functions can be outsourced** to external contractor(s) with particular expertise.


Cybersecurity Architect
+
Cybersecurity Implementer
Outsource functions to external Contractor(s)
01010
11101
00101

Product as a Service

Based on Organisation's needs

✓ **Plan, design, and implement security solutions and controls**

- Plan and build secure networks and ensure a secure environment throughout the development process.
- 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 solutions within the specified time to address and fix issues identified during security audits.

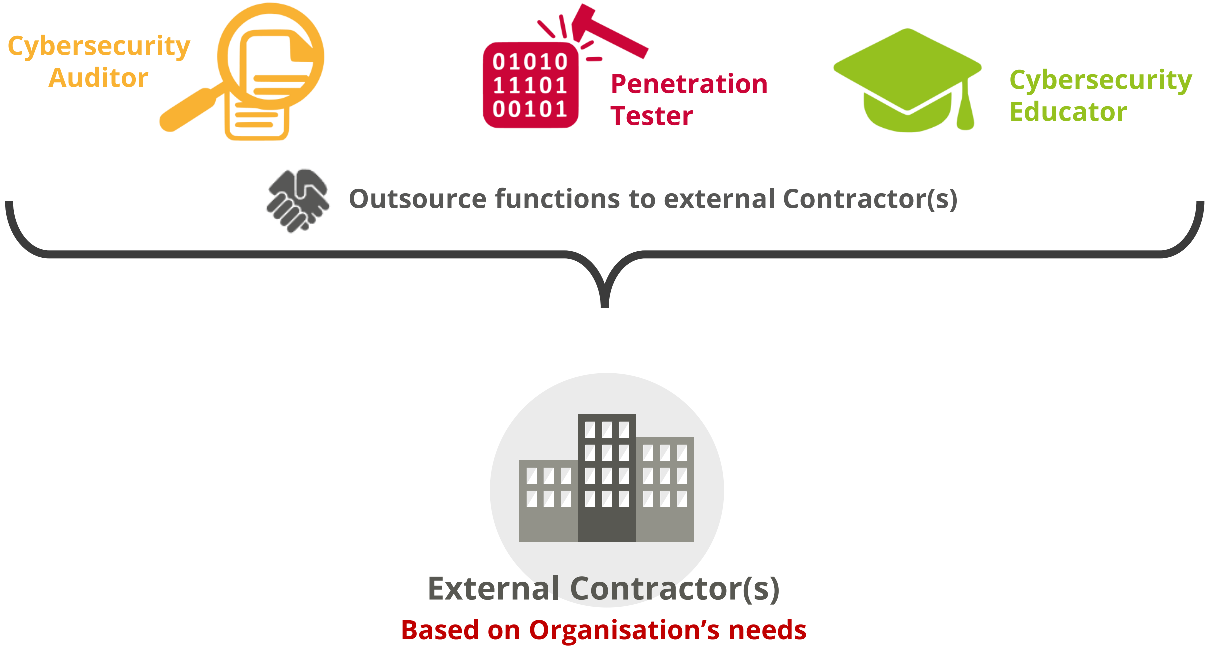
Using ECSF we can draft the needed tasks outsource them to the appropriate experts.

EXAMPLE

OUTSOURCING FUNCTIONS

REQUIREMENTS STEMMING FROM NIS2

Some **occasional used functions can be outsourced** to external contractor(s) with particular expertise.



Cybersecurity Auditor

Penetration Tester

Cybersecurity Educator

Outsource functions to external Contractor(s)

External Contractor(s)

Based on Organisation’s needs

Using ECSF we can draft the needed tasks outsource them to the appropriate experts.

✓ Ensure compliance through Cybersecurity Audits

- Perform audits to ensure the company follows cybersecurity training, risk measures, and reporting obligations.
- Conduct internal audits and provide reports to authorities when requested.

✓ Conduct vulnerability assessment test

- 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.
- Assists the competent authorities' personnel on the security scans conducted.

✓ 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.

THANK YOU FOR YOUR ATTENTION

Agamemnonos 14, Chalandri 15231
Attiki, Greece

info@enisa.europa.eu

www.enisa.europa.eu