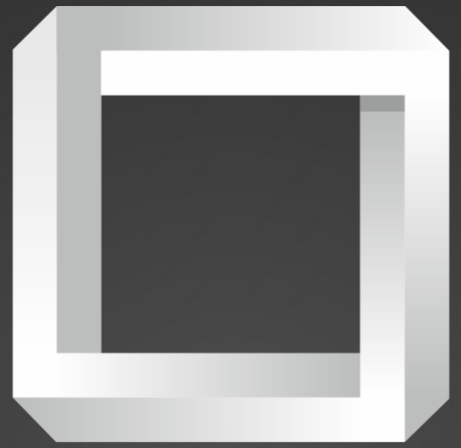


CYBERFLIP

Cybersecurity for Next Generation Enterprises

Cyber Resilience Services - NIS 2

December 2024

Contents

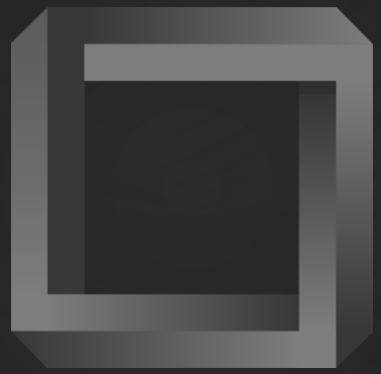
CYBERFLIP

NIS 2

- NIS 2 Directive
- NIS Vs NIS 2
- Sectors
- Measures

Our Approach

- Services
- Services Bundles
- Your Journey Towards NIS 2 Compliance



NIS 2 Directive

NIS 2 Directive

CYBERFLIP

- The NIS 2 Directive refers to the European Union's Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union.
- It was introduced in 2020 and came into effect on January 16, 2023.
- Aims to enhance the EU's cybersecurity framework by requiring operators of critical infrastructure and essential services to implement appropriate security measures and report any incidents to the relevant authorities.
- Transposed into the Greek Law 2024/5160 on 27/11/2024

NIS vs NIS 2

CYBERFLIP

NIS

- Cybersecurity Directive by the EU introduced in 2016
- Aims to enhance the security of network and information systems within the EU
- Requires operators of critical infrastructure and essential services to:
  - Implement appropriate security measures
  - Report any incidents to the relevant authorities

VS

NIS 2

- Expansion of NIS
- Fixes challenges and inconsistencies that came up in the first version
- Expands security requirements and the scope of covered organizations
- Introduces new sectors (15 compared to 7)
- Simplifies reporting obligations
- Enforces more stringent measures & sanctions throughout Europe: Legal ramifications introduced in addition to heavy fines for non-compliance

NIS 2 Management Responsibilities

CYBERFLIP

- Approves the adequacy of the cybersecurity risk management measures taken by the entity
- Supervise the implementation of the risk management measures
- Follow training in order to gain sufficient knowledge and skills to identify risks and assess cybersecurity management practices and their impact on the services provided the entity
- Offer similar training to their employees on a regular basis
- Be accountable for the non-compliance

NIS 2 Penalties

CYBERFLIP

Non-Monetary penalties

Such as compliance orders, binding instructions, security audit implementation orders

Administrative fines

maximum value of at least €10.000.000 or 2% of the global annual revenue for essential entities, and at least €7.000.000 or 1,4% of the global annual revenue for important entities

Criminal Sanctions for management

These penalties can be imposed on essential entities and important entities for infractions such as failure to meet security requirements and failure to report incidents

Sectors

CYBERFLIP

Sector Covered by NIS 2

2 Distinct Categories:

Essential Entities	Important Entities

Entities in both categories will have to meet the same requirements.

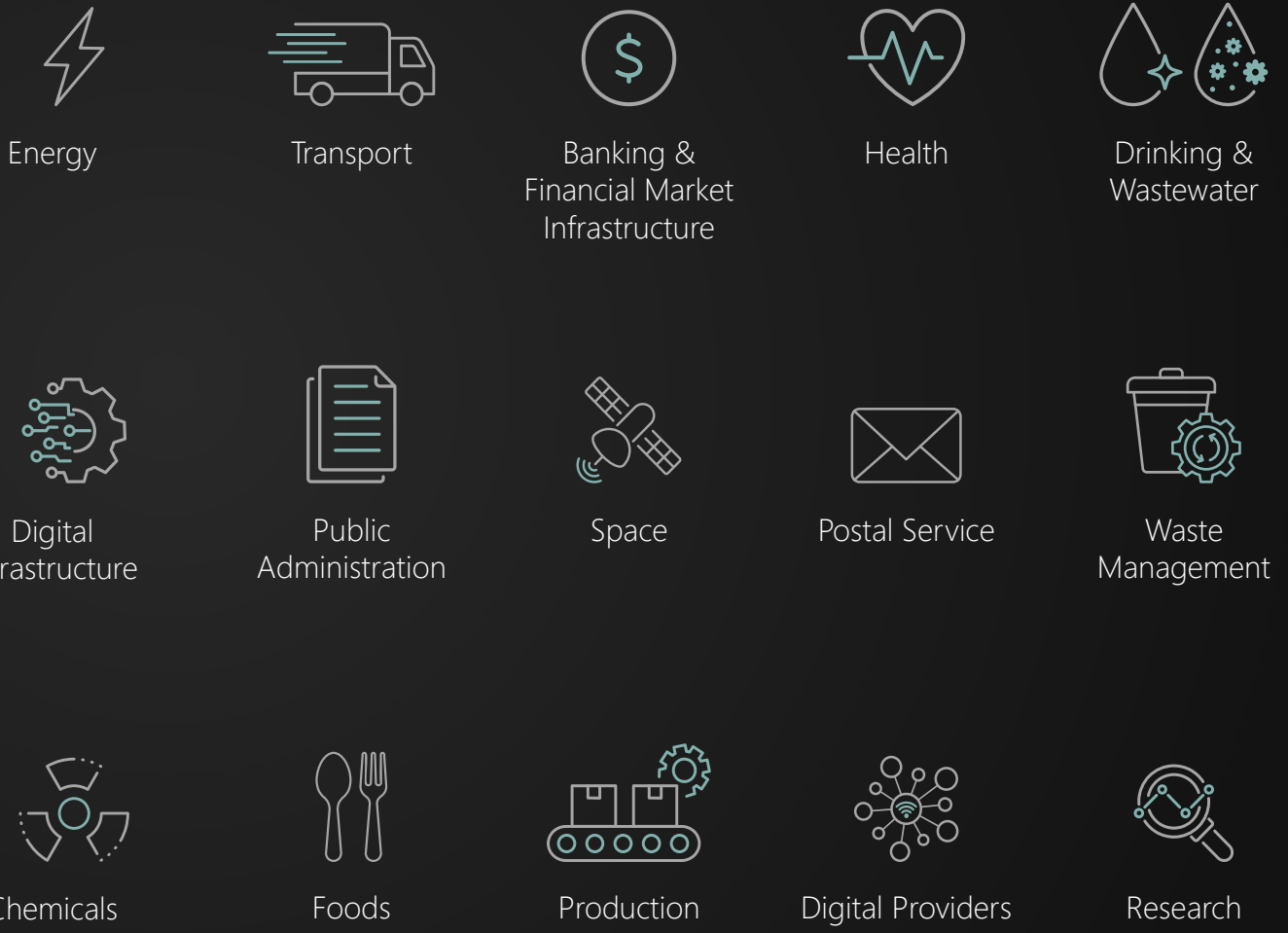
However:

Essential entities will be more tightly controlled and sanctioned.

Essential entities will be required to meet supervisory requirements as of the introduction of NIS2. Also, higher sanctions are applied.

Important entities will be subject to ex-post supervision, in case of evidence of non-compliance.

No more categorization of OES and DSP



Sectors

CYBERFLIP

Sector Covered by NIS 2

Sectors of high criticality	Size thresholds
▪ Energy ▪ Transport ▪ Finance ▪ Public Administration ▪ Health ▪ Space ▪ Water Supply ▪ Digital Infrastructure	▪ 250 employees or more than €50 million revenue: **Essential** ▪ 40-249 employees or more than 10M revenue: **Important** ▪ Specific subcategories of Digital Infrastructure are considered always **Essential** ▪ Public Administration is considered in most cases **Essential** (exemptions apply)

Energy

Transport

Banking & Financial Market Infrastructure

Health

Drinking & Waste Water

Digital Infrastructure

Public Administration

Space

Postal Service

Waste Management

Chemicals

Foods

Production

Digital Providers

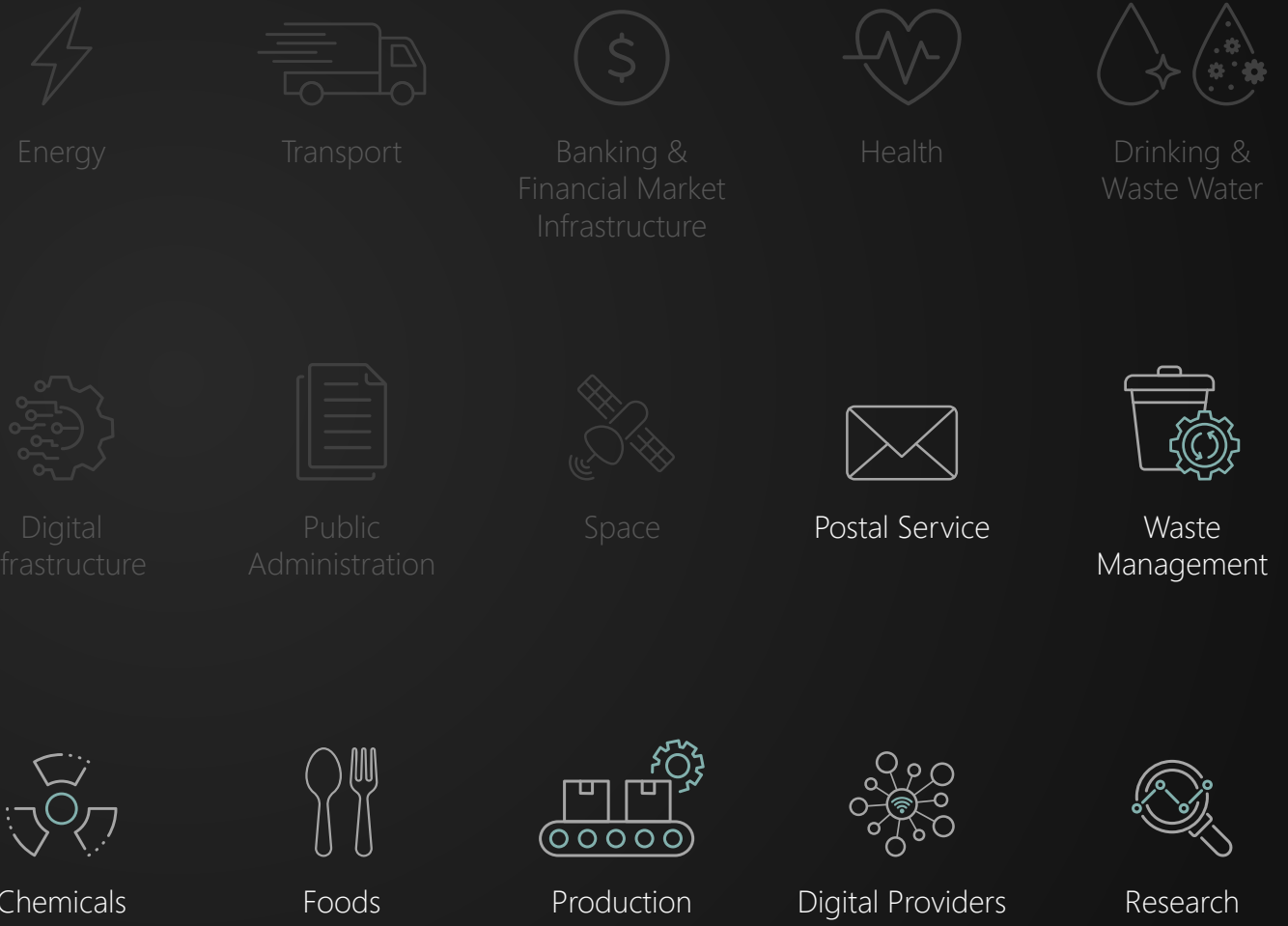
Research

Other Critical Sectors

CYBERFLIP

Sector Covered by NIS 2

Important Entities	Size thresholds
▪ Postal Services ▪ Waste Management ▪ Chemicals ▪ Research ▪ Foods ▪ Manufacturing ▪ Digital Providers ▪ Entities providing Domain Name Registration Services (all sizes, but only subject to Article 3(3) and Article 28)	▪ 250 employees or more than €50 million revenue: Important ▪ 40-249 employees or more than 10M revenue: Important



Measures

CYBERFLIP

Cybersecurity Risk Management Measures Article 21

a) Policies framework and risk analysis

b) Incident handling

c) Crisis management and business continuity

d) Supply chain security

e) Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure

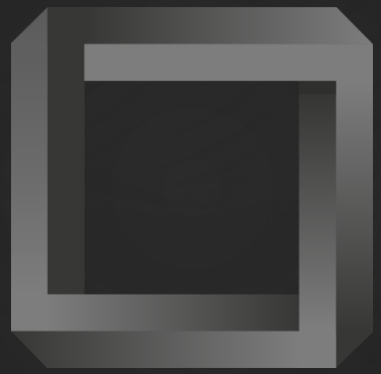
f) Policies and procedures (testing and auditing) to assess the effectiveness of cybersecurity risk management measures

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



Our Approach

Services

CYBERFLIP

End-to-end Security and Compliance

- Tailored solutions ensuring smooth integration of technology and associated policies and procedures.
- Ongoing compliance covering efficiently all requirements.

Services

CYBERFLIP

Addressing NIS 2 Requirement

NIS 2 Requirement	GRC Services
1. Policies framework and risk analysis	IS Framework Risk Assessment
2. Incident Handling	IS Framework Incident Response Playbooks
3. Crisis management and business continuity	BCMS Crisis Management
4. Supply chain security	IS Framework Technical Security Assessments
5. Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	IS Framework Technical Security Assessments

CYBERFLIP

Addressing NIS 2 Requirement

NIS 2 Requirement	GRC Services
6. Policies and procedures for testing and auditing	IS Framework Internal audits & Maturity Assessment Technical Security Assessments IR & Crisis Simulation
7. Basic cyber hygiene practices and cybersecurity training	IS Framework Cyber awareness training Phishing simulations
8. Policies and procedures regarding the use of cryptography and, where appropriate, encryption	IS Framework
9. Human resources security, access control policies and asset management	IS Framework Risk Assessment User roles review and SoD Review
10. MFA and authentication measures	IS Framework

Services Bundles

CYBERFLIP

Choose what you Need or Build your Custom Bundle

Fundamental	Optimum	Full	Custom
Gap Analysis & Risk Assessment	All services of Fundamental	All Services of Optimum	Build your own service bundle based on your needs
Information Security Framework	Incident Response Playbooks	Incident Response & Crisis Simulation	
BCMS Design	Awareness training & Phishing	User Roles and SoD review	
IR & Crisis Management	Red teaming	Internal Audit	
Penetration Test and Vulnerability Assessment			

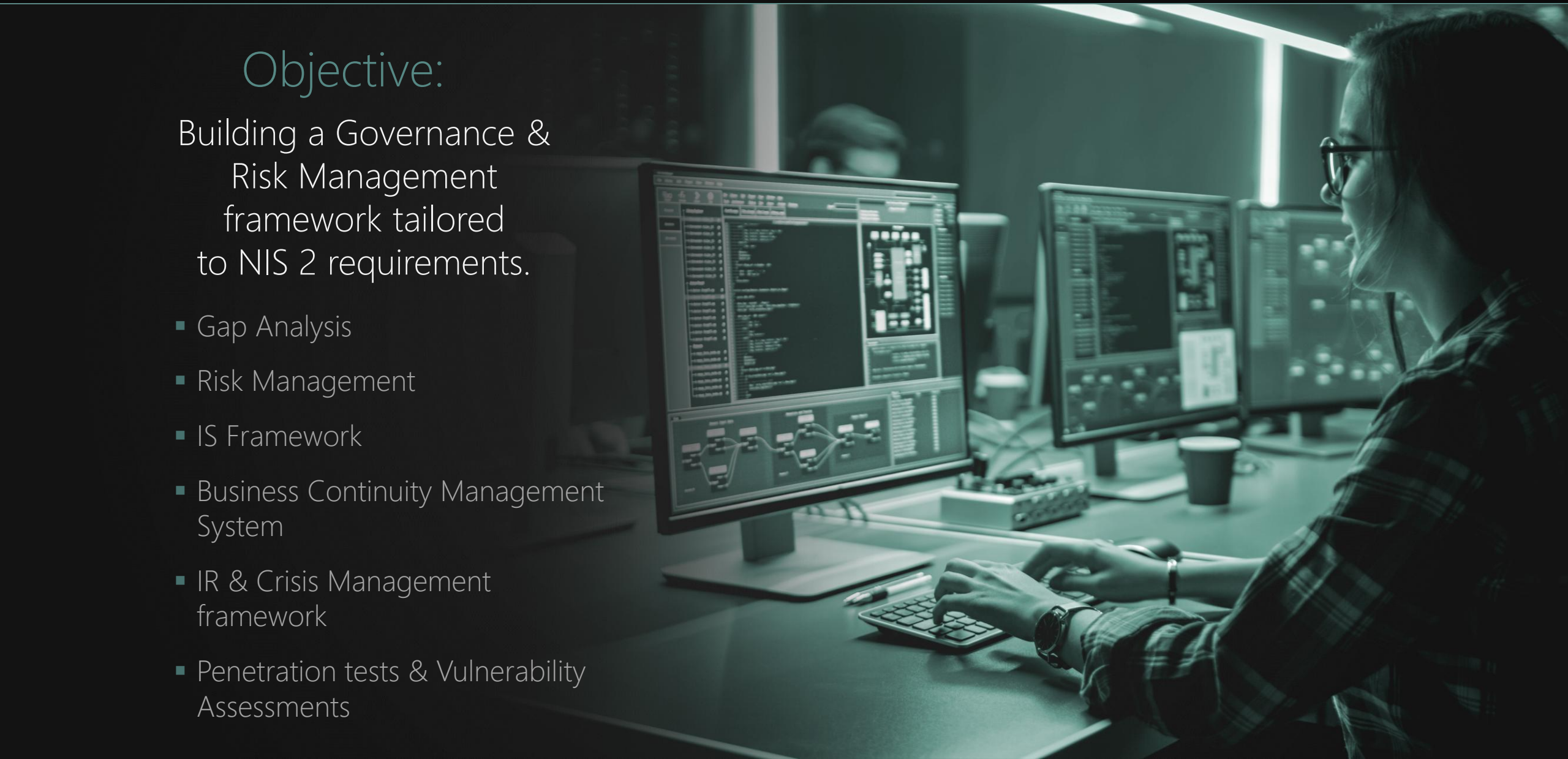
Fundamental Services

CYBERFLIP

Objective:

Building a Governance & Risk Management framework tailored to NIS 2 requirements.

- Gap Analysis
- Risk Management
- IS Framework
- Business Continuity Management System
- IR & Crisis Management framework
- Penetration tests & Vulnerability Assessments



Fundamental Services

CYBERFLIP

Cyber Risk Management & IS Framework

"How to efficiently manage all these requirements?"

Gap Analysis & Risk Assessment

Need

Transform a list of requirements into tailored accurately prioritized actions.

Solution

Quantitative approach to transform Risk Assessment into a decision-making tool bridging the gap between technology, regulatory requirements and business objectives.

NIS 2 Requirements:
✓ **All**

IS framework

Need

Efficiently integrate compliance requirements into everyday business.

Solution

Design a tailored framework based on NIS 2 requirements and unique operational or additional regulatory needs for each Organization.

NIS 2 Requirements:
✓ **All**

Fundamental Services

CYBERFLIP

Cyber Resilience

"How to feel confident that you will survive?"

BCMS Design

Need

Focus on what actually "runs the business".

Solution

Pragmatic approach to identify the "crown jewels" and build the BC capability around them.

NIS 2 Requirements:
✓ 3

IR and Crisis Management Framework

Need

Not only being able to respond but feel confident that Crisis is managed.

Solution

Design a specific framework with pre-defined responsibilities of internal and external parties harmonically integrating technical and non-technical roles.

NIS 2 Requirements:
✓ 2,3

CYBERFLIP

Technical Assessments

"How to ensure actual implementation of technical controls?"

Penetration tests and Vulnerability Assessments

Need

Ensure that technical implementations are secure.

Solution

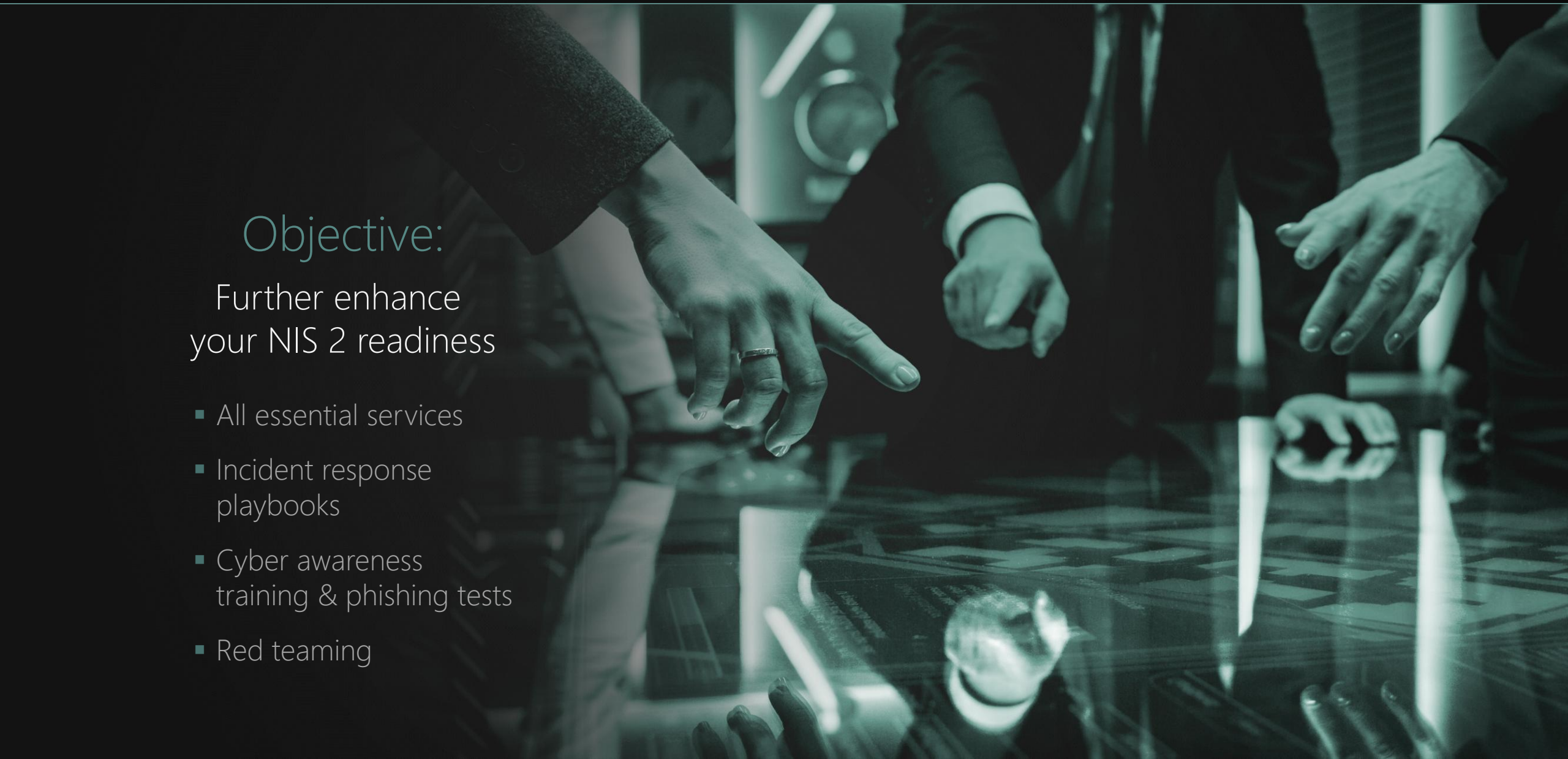
Tailored tests from experienced ethical hackers with clear and defined scope utilizing latest trends.

NIS 2 Requirements:

✓ **4,5,9**

Optimum Services

CYBERFLIP



Objective:

Further enhance your NIS 2 readiness

- All essential services
- Incident response playbooks
- Cyber awareness training & phishing tests
- Red teaming

CYBERFLIP

Incident Response Capability

"Define your threats. Define your response holistically"

Incident Response Playbooks

Need	Solution
Being able to handle specific incidents efficiently.	Specific playbooks, tailored to each industry covering end-to-end response and recovery including technical and non-technical roles on the same frame.

NIS 2 Requirements:

✓ 2

Optimum Services

CYBERFLIP

Cyber Awareness

"How to build real awareness?"

Cyber Awareness & Phishing simulations

Need

Re-gain user interest to achieve real awareness and enhance the most important control – human factor.

Solution

Tailored training program including a blend mix of multimedia, classrooms and social engineering tests, fitted to each Organization's unique profile.

NIS 2 Requirements:

✓ **7**

Optimum Services

CYBERFLIP

Be the attacker

"What if a malicious hacker targets your Organization?"

Red teaming

Need

Investigate how deep a malicious hacker could reach and what the real impact could be

Solution

Run zero-knowledge hacking exercises from experienced ethical hackers and test in practice your security controls

NIS 2 Requirements:

✓ **4,5,9**

Full Services

CYBERFLIP

Objective:

Assess your readiness

- All Optimum services
- Incident & Crisis response simulation
- User roles and SoD review
- Internal audit

Full Services

CYBERFLIP

Simulate

"Are you ready to respond?"

Incident response simulations

Need

Experience a real-world scenario and test actual readiness.

Solution

Simulate playbooks utilizing a combined exercises that involves the participation of all roles.

NIS 2 Requirements:
✓ 2 , 6

Crisis simulations

Need

Feel confidence to manage crisis on real world scenarios.

Solution

Mutually design a real-world scenario and monitor Organization's performance over handling a crisis.

NIS 2 Requirements:
✓ 3

Full Services

CYBERFLIP

User Access Security

"Take control of who actually needs to perform what with the minimum risk"

User access roles and SoD review

Need

User access inconsistencies remains a major vulnerability globally.

Solution

Drive business and technology to identify actual roles needs and resolve potential conflicts.

NIS 2 Requirements:

✓ **9**

Full Services

CYBERFLIP

Monitor and Improve

"Take control of your ongoing compliance Journey"

Internal Audit

Need	Solution
Define the exact level of readiness.	A blended team of seasoned and talented professionals that will provide an end-to-end assurance based on specific and pre-agreed audit steps.

NIS 2 Requirements:

✓ **6**

Your Journey Towards NIS 2 Compliance

CYBERFLIP

Initial Phase (Steps 1,2)

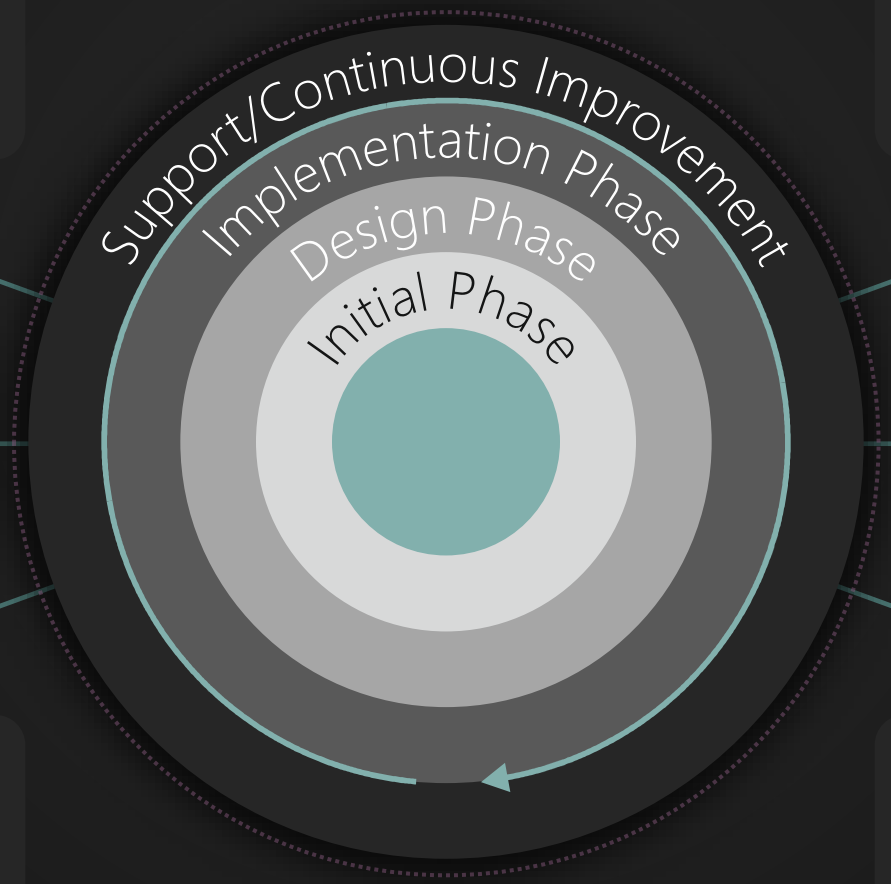
Identifying status (Gap analysis) and prioritize needed actions (Risk Assessment).

Fundamental bundle

Implementation Phase (Step 4)

Guide the Organization into integrating security into daily operations.

Fundamental, Optimum bundle



STEP 1 Gap Analysis

STEP 2 Risk Assessment

STEP 3 Design

STEP 4 Implementation

STEP 5 Review

STEP 6 Improvement

Design Phase (Step 3)

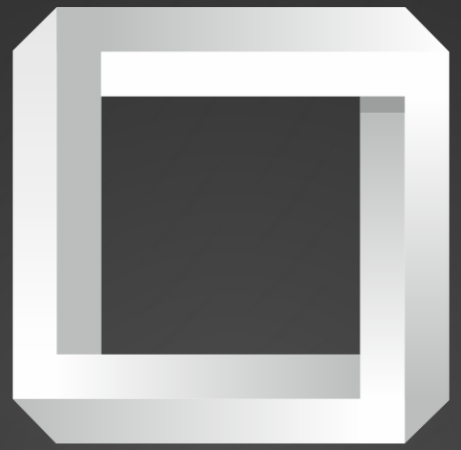
Design of an NIS 2 compliant framework, tailored to Organization's unique needs.

Fundamental bundle

Continuous Improvement (Steps 5,6)

Activities for maintaining and improving compliance levels in the most efficient manner.

Full bundle



CYBERFLIP

Cybersecurity for Next Generation Enterprises

Thank you!