Embracing ISO27001

Roadmap to Compliance for INEX

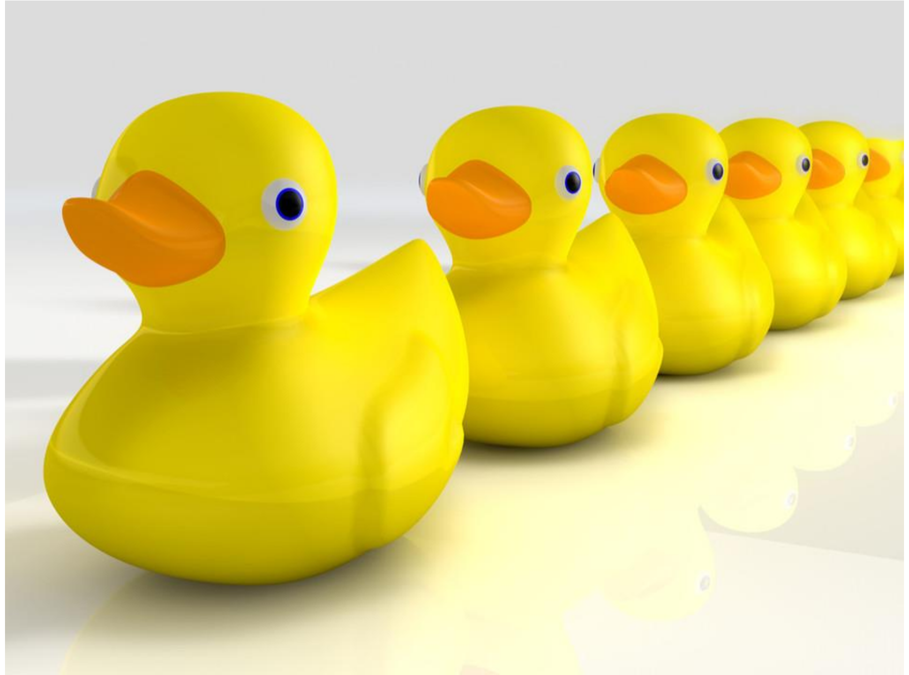
Eileen Gallagher and Barry O’Donovan

INTERCONNECTING NETWORKS AND PEOPLE FOR OVER 25 YEARS

INEX

INTERCONNECTING NETWORKS
AND PEOPLE FOR OVER 25 YEARS

Two Types of Organisations



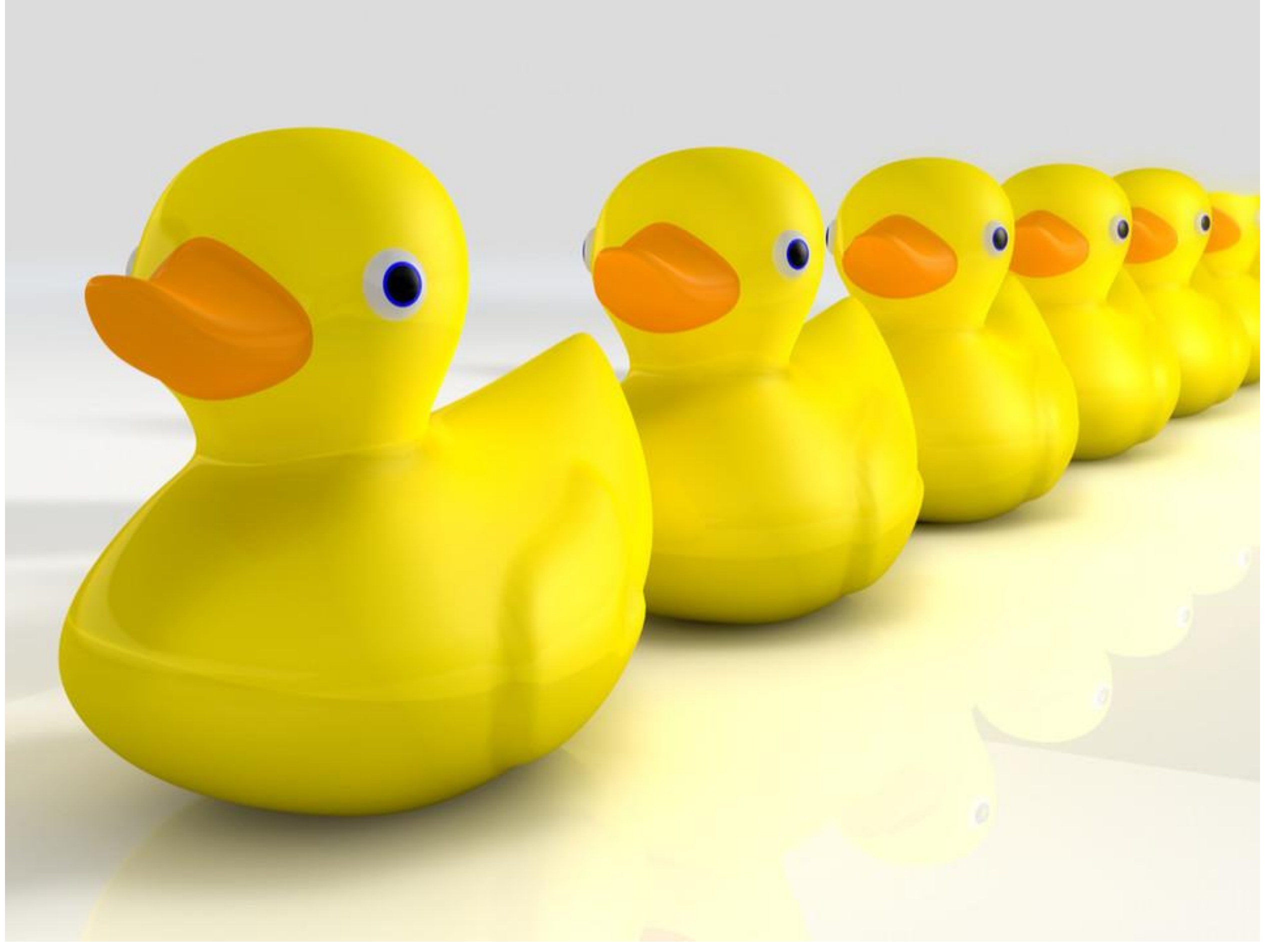
- Formal processes in place
- Have been implementing some degree of security best practice

- Ad hoc approach
- Busy building/scaling the business with little focus on security

INEX Commitment to Security

- Long term focus on robust security practices at INEX
- Critical to ensuring resilient and secure environment for our members
- We accept our place in delivering vital network infrastructure
- Evolving cybersecurity regulation and approach meant we had to review our ‘posture’ in this area
- NIS1 and NIS2 hugely impactful in our industry and those we serve
- **Most important:** our commitment is driven by our focus on delivering reliable, scalable and secure network infrastructure that our members depend on

INEX



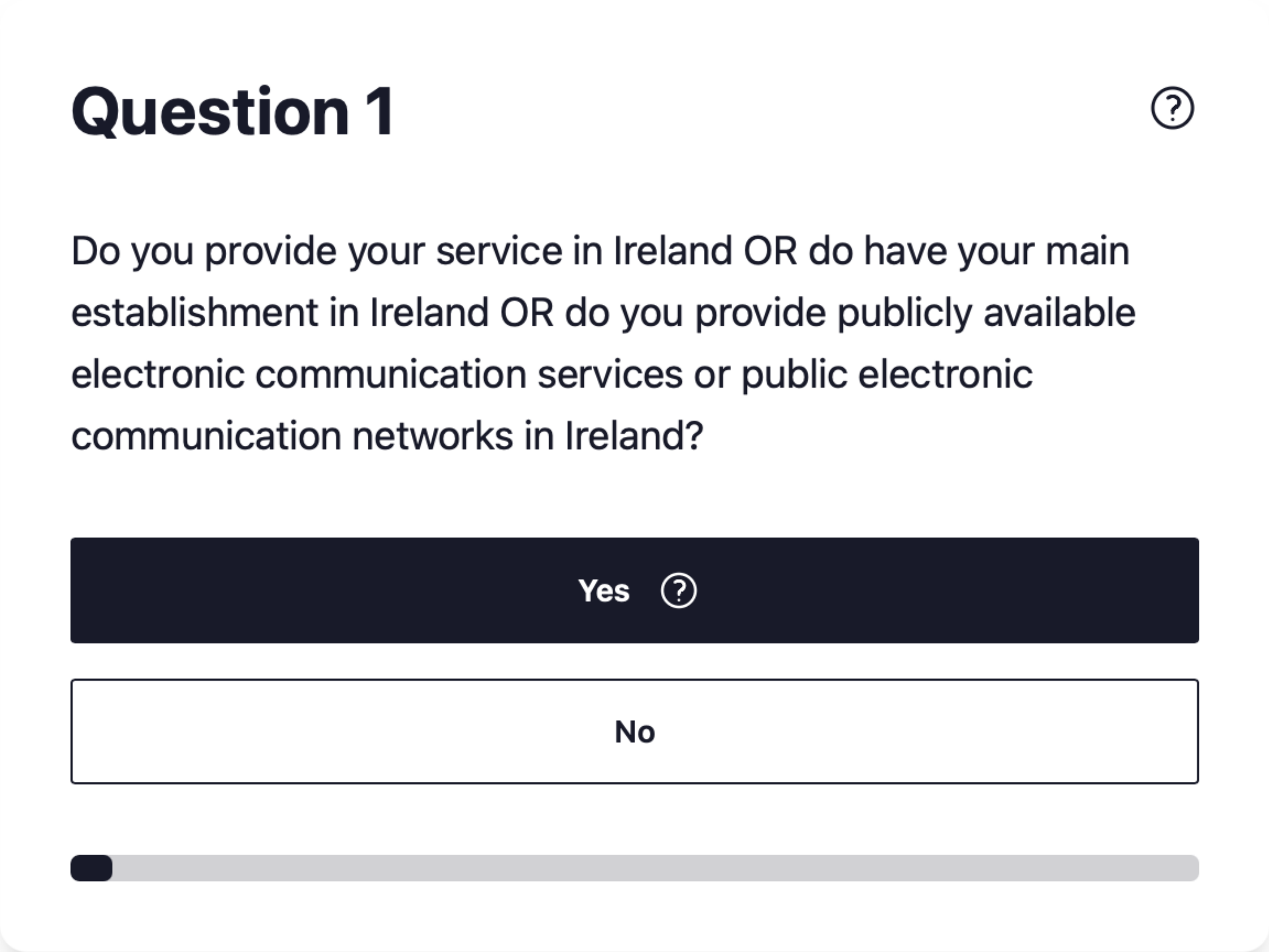
NIS2 on the Horizon

NIS1 / NIS2 and INEX

- INEX was not included in NIS1
- INEX is not in scope for NIS2 (small entity exception)
- NIS2 not fully transposed into primary legislation in Ireland
  - The Heads of Bill published in September
  - Election now called – unlikely to see it before mid-2025
- National Cyber Security Centre published a tool:
  - https://www.ncsc.gov.ie/nis2/amiinscope/
- Already aligned if brought into scope in the future

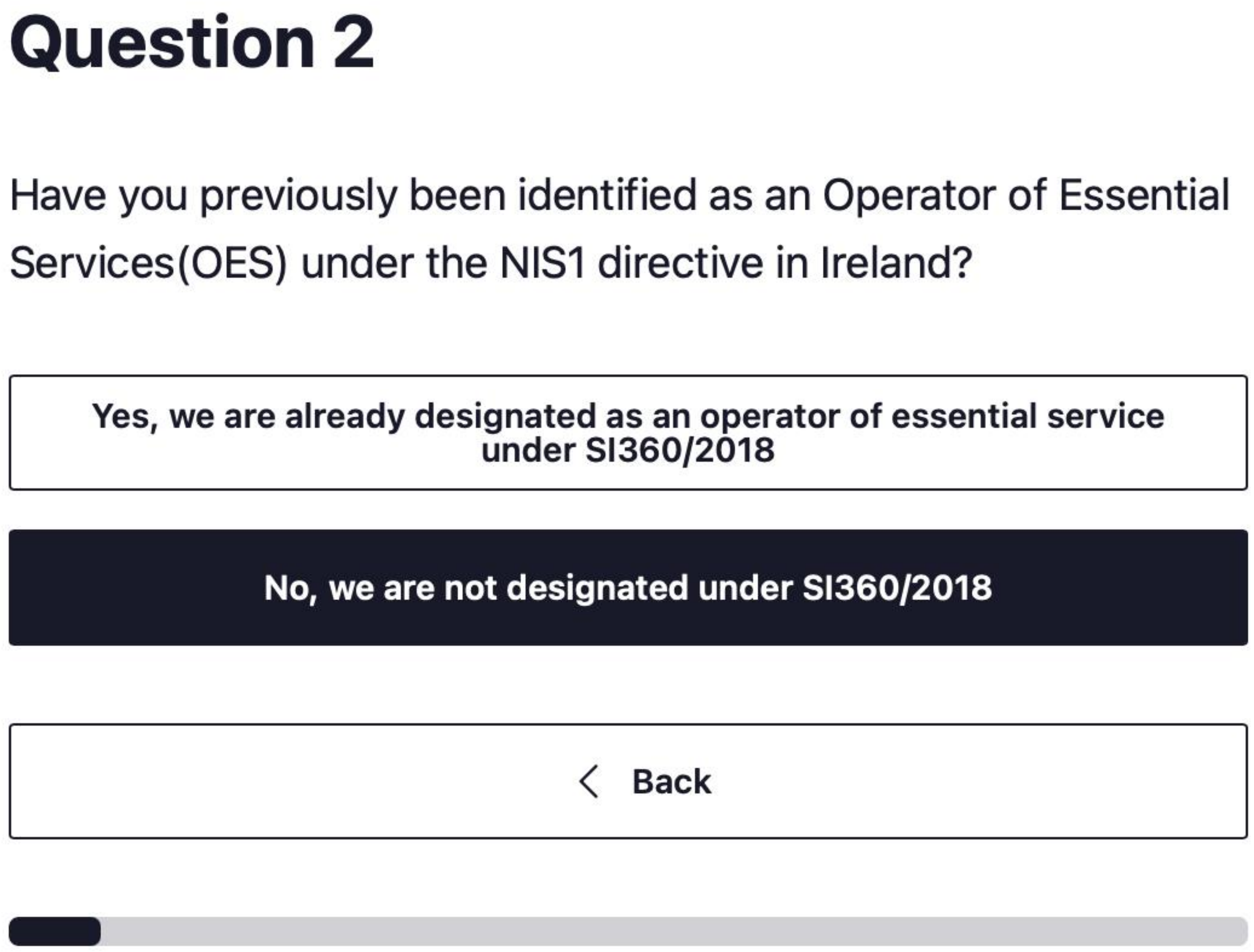
NIS2

AM I IN SCOPE?



Question 1

Do you provide your service in Ireland OR do have your main establishment in Ireland OR do you provide publicly available electronic communication services or public electronic communication networks in Ireland?

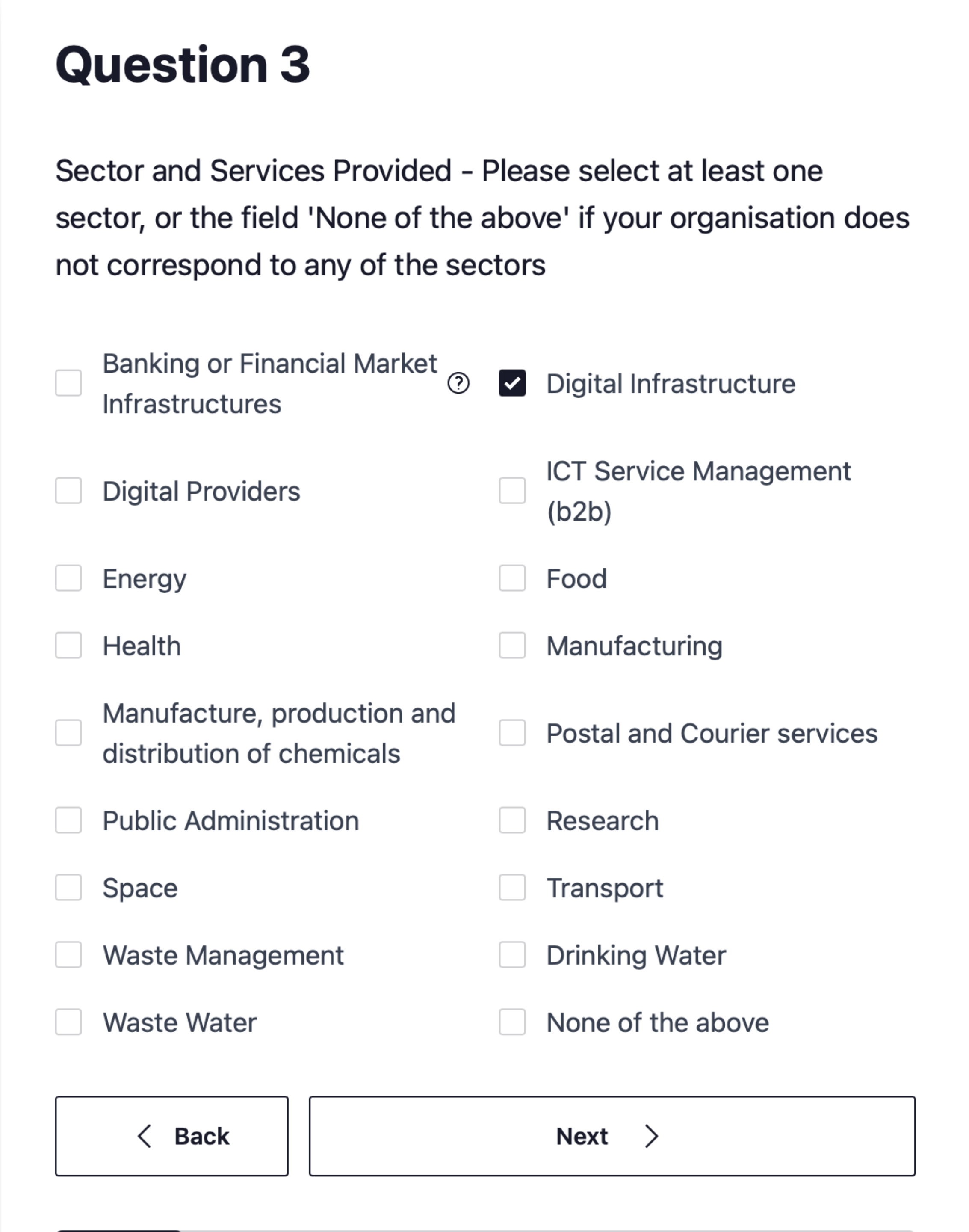


Question 2

Have you previously been identified as an Operator of Essential Services(OES) under the NIS1 directive in Ireland?

Yes, we are already designated as an operator of essential service under SI360/2018

No, we are not designated under SI360/2018



Question 3

Sector and Services Provided - Please select at least one sector, or the field 'None of the above' if your organisation does not correspond to any of the sectors

□ Banking or Financial Market Infrastructures ⓘ

☑ Digital Infrastructure

□ Digital Providers

□ ICT Service Management (b2b)

□ Energy

□ Food

□ Health

□ Manufacturing

□ Manufacture, production and distribution of chemicals

□ Postal and Courier services

□ Public Administration

□ Research

□ Space

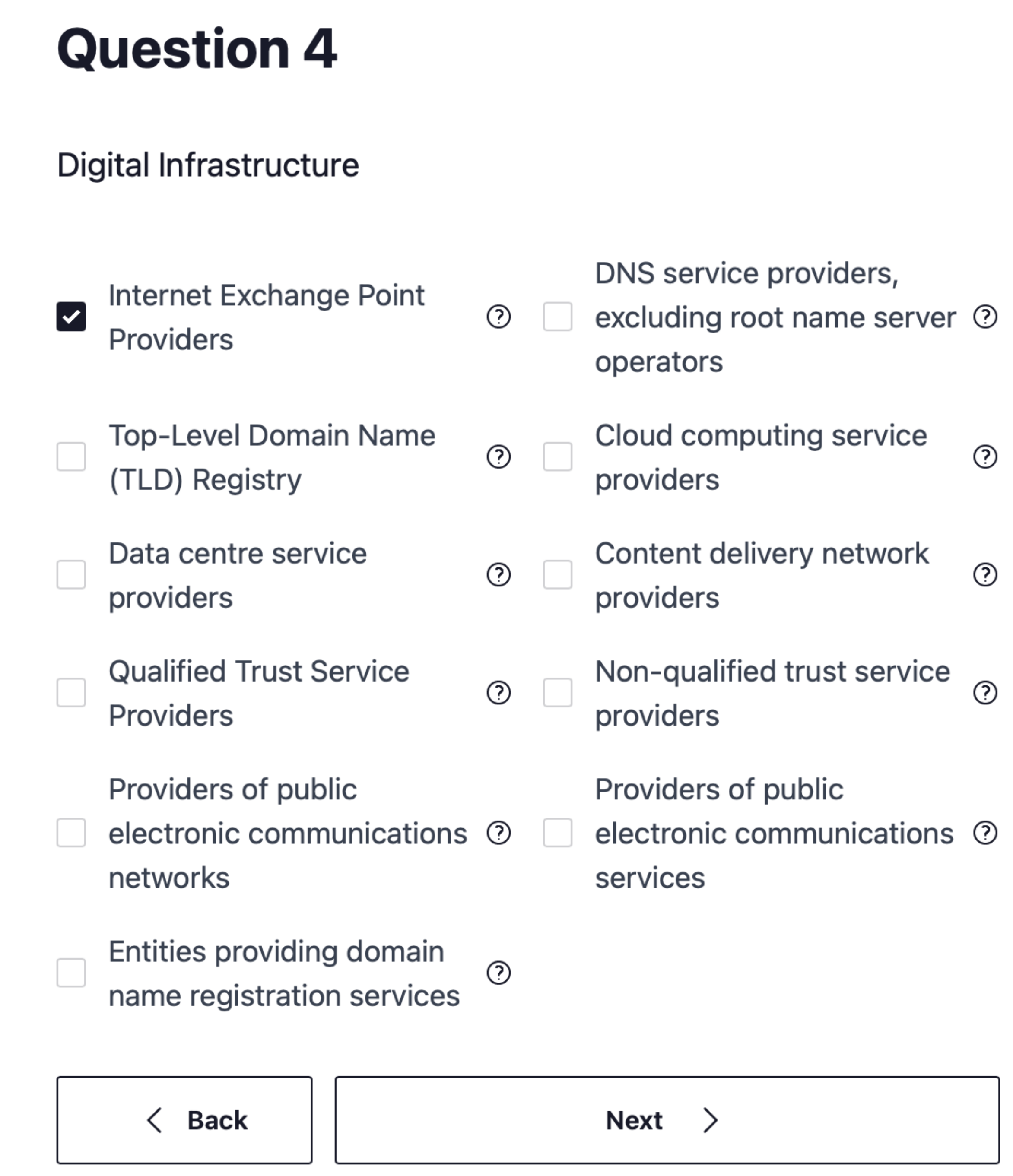
□ Transport

□ Waste Management

□ Drinking Water

□ Waste Water

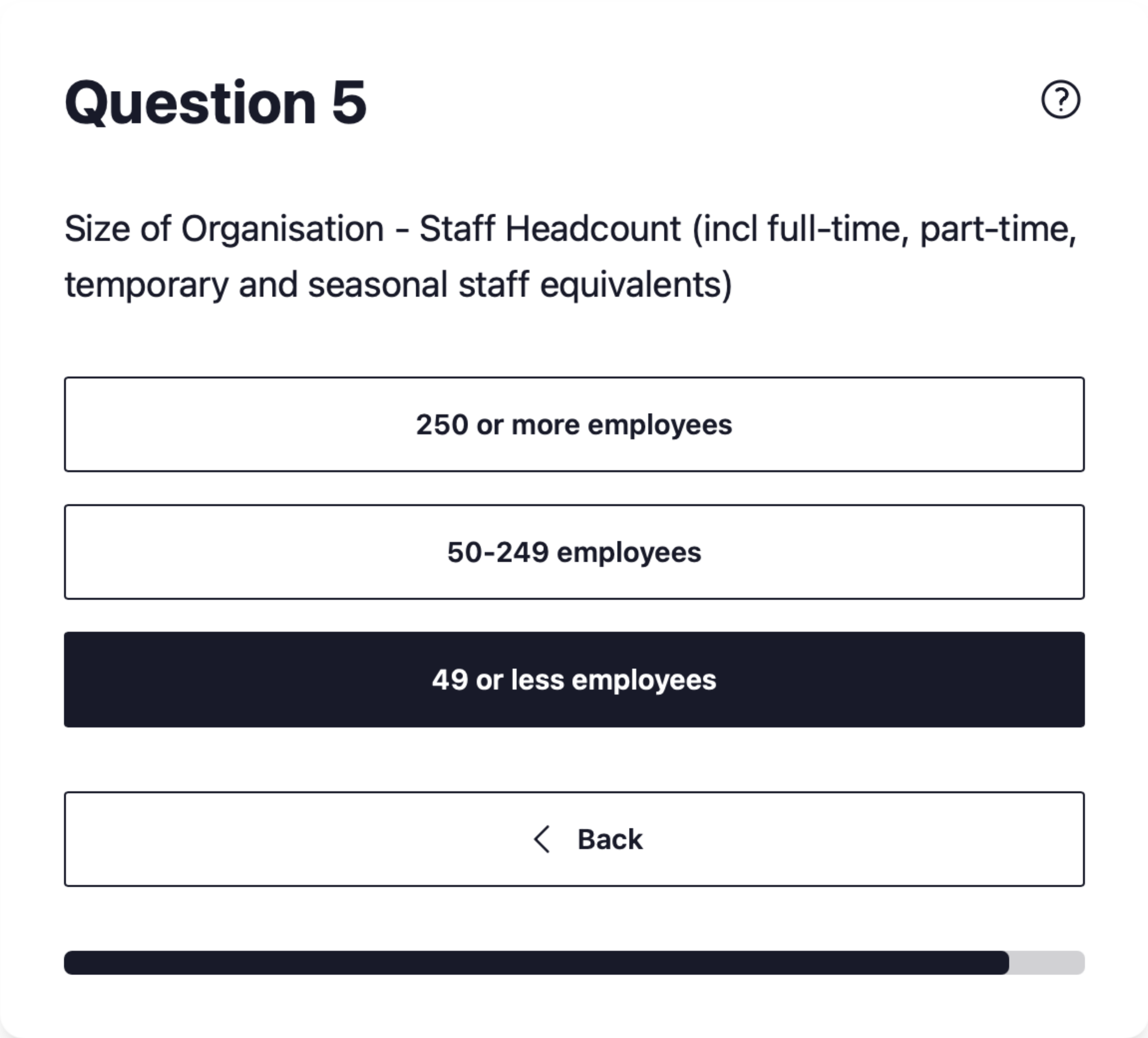
□ None of the above



Question 4

Digital Infrastructure

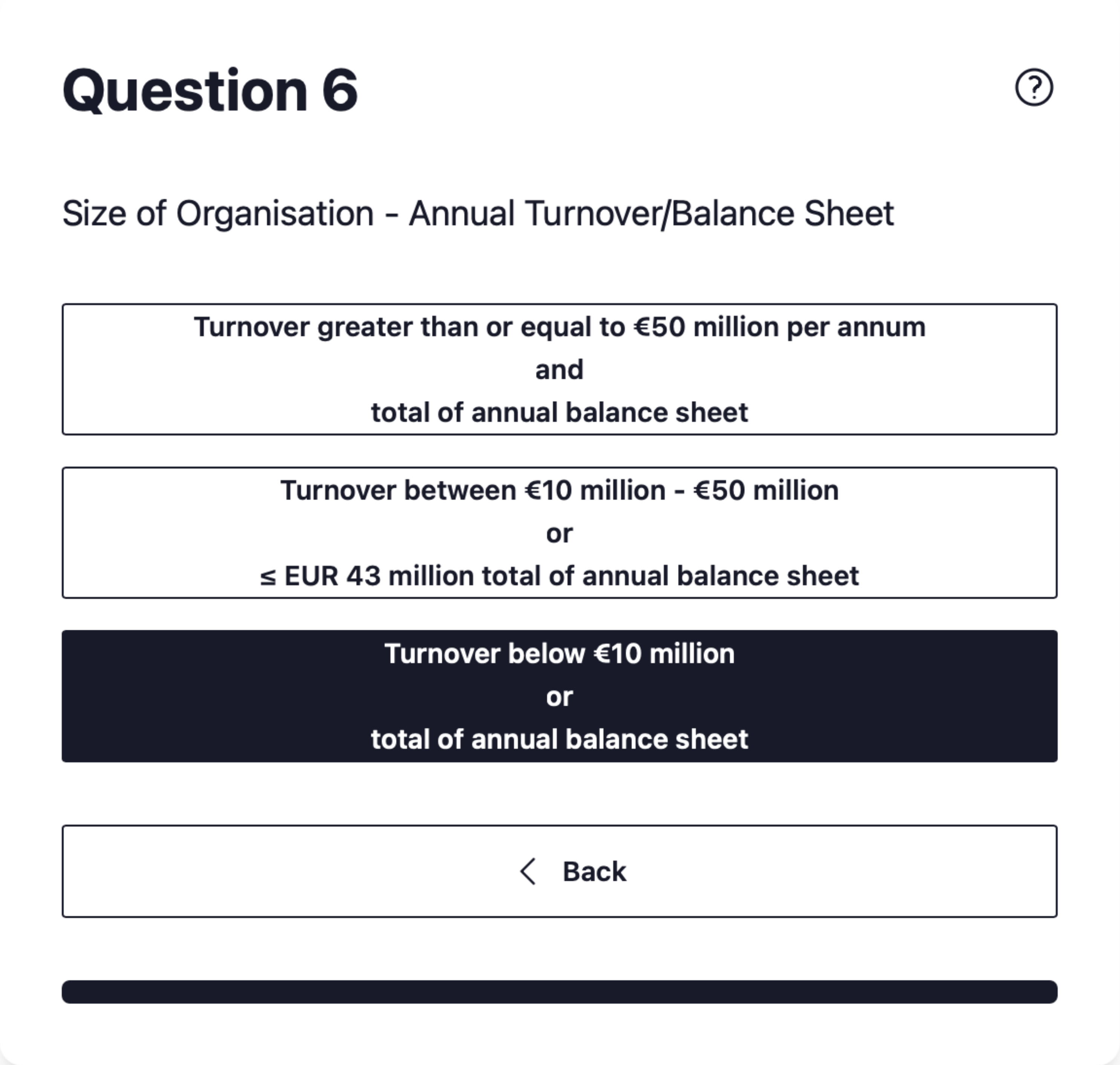
- ☑ Internet Exchange Point Providers ⓘ
- □ Top-Level Domain Name (TLD) Registry ⓘ
- □ Data centre service providers ⓘ
- □ Qualified Trust Service Providers ⓘ
- □ Providers of public electronic communications networks ⓘ
- □ Entities providing domain name registration services ⓘ
- □ DNS service providers, excluding root name server operators ⓘ
- □ Cloud computing service providers ⓘ
- □ Content delivery network providers ⓘ
- □ Non-qualified trust service providers ⓘ
- □ Providers of public electronic communications services ⓘ



Question 5

Size of Organisation - Staff Headcount (incl full-time, part-time, temporary and seasonal staff equivalents)

- 250 or more employees
- 50-249 employees
- [✓ 49 or less employees]



Question 6

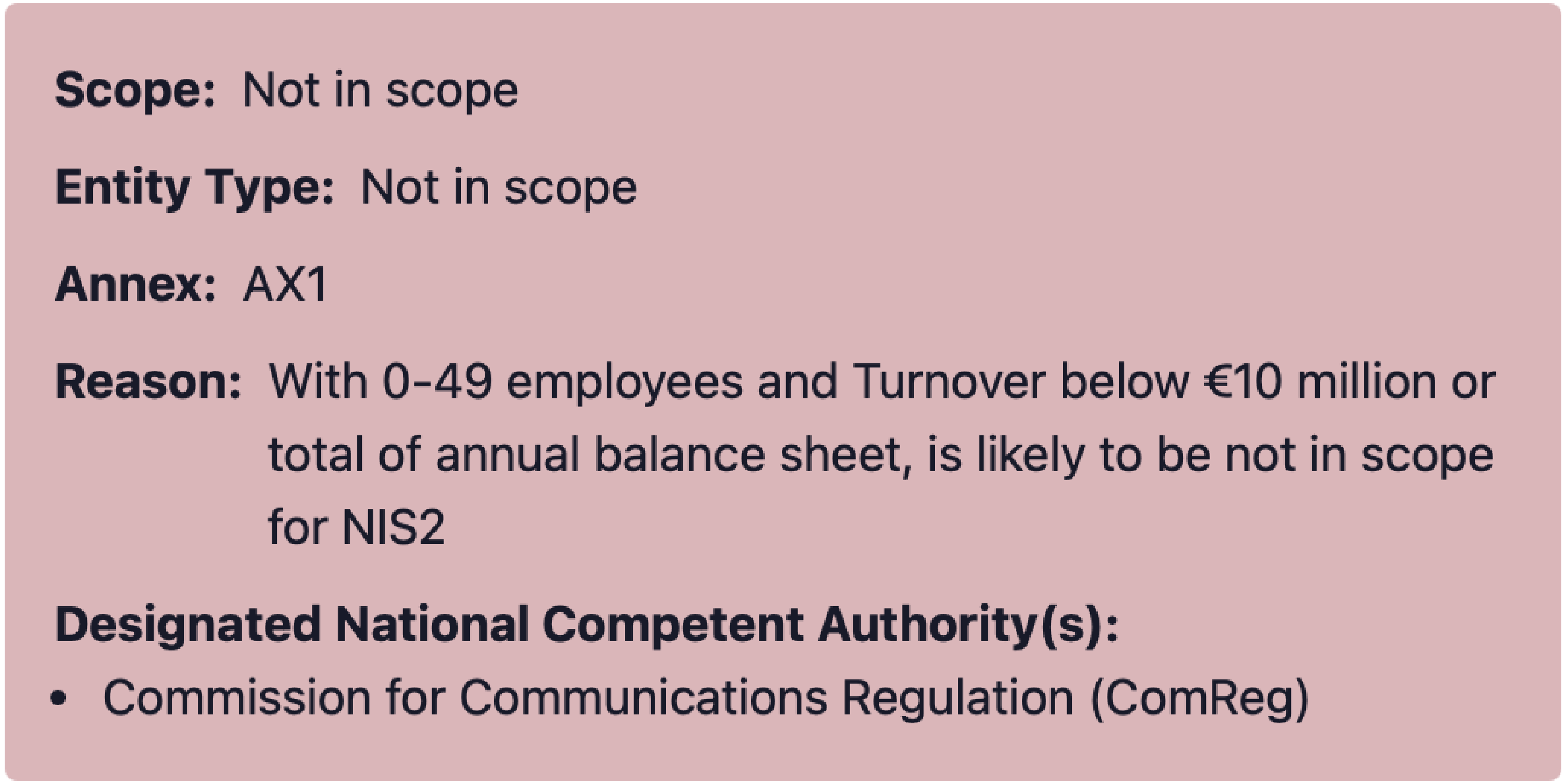
Size of Organisation - Annual Turnover/Balance Sheet

Turnover greater than or equal to €50 million per annum
and
total of annual balance sheet

Turnover between €10 million - €50 million
or
≤ EUR 43 million total of annual balance sheet

[✓ Turnover below €10 million
or
total of annual balance sheet]

Result



Scope: Not in scope

Entity Type: Not in scope

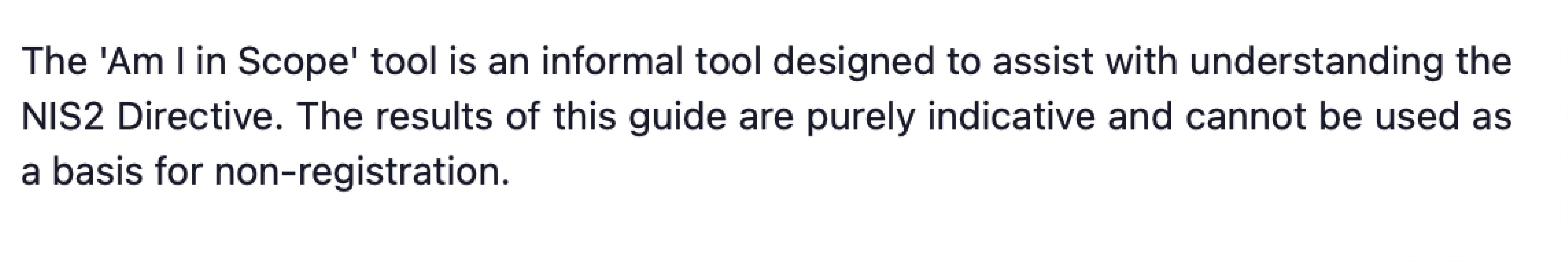
Annex: AX1

Reason: With 0-49 employees and Turnover below €10 million or total of annual balance sheet, is likely to be not in scope for NIS2

Designated National Competent Authority(s):

- Commission for Communications Regulation (ComReg)

Health Warning



The 'Am I in Scope' tool is an informal tool designed to assist with understanding the NIS2 Directive. The results of this guide are purely indicative and cannot be used as a basis for non-registration.

Business Drivers and Approach

The Business Decision

- Proactive, ongoing risk management and regulatory alignment
  - Gave us a structured approach to avoiding ‘one and done’
  - Very likely that ISO27001 will evolve inline with regulatory developments
- Valuable self assessment mirror helping to identify vulnerabilities and push us out of the comfort zone
  - Reflected our approach of continuous improvement INEX was very keen to lead by example in this area
- Leading by example was important
  - Conscious that all our members are facing similar challenges
- Member trust is critical in our network and security
  - ISO27001 Certification serves to safeguard that trust
- External validation with ISO27001 Certification
  - Third party endorsement of our secure and robust approach to designing, delivering and managing the INEX infrastructure

Stage 1- Gap Analysis to NIS1 “What is the state of the Nation?”

People

- Management oversight
- Staff awareness training
- Key person risk

Process

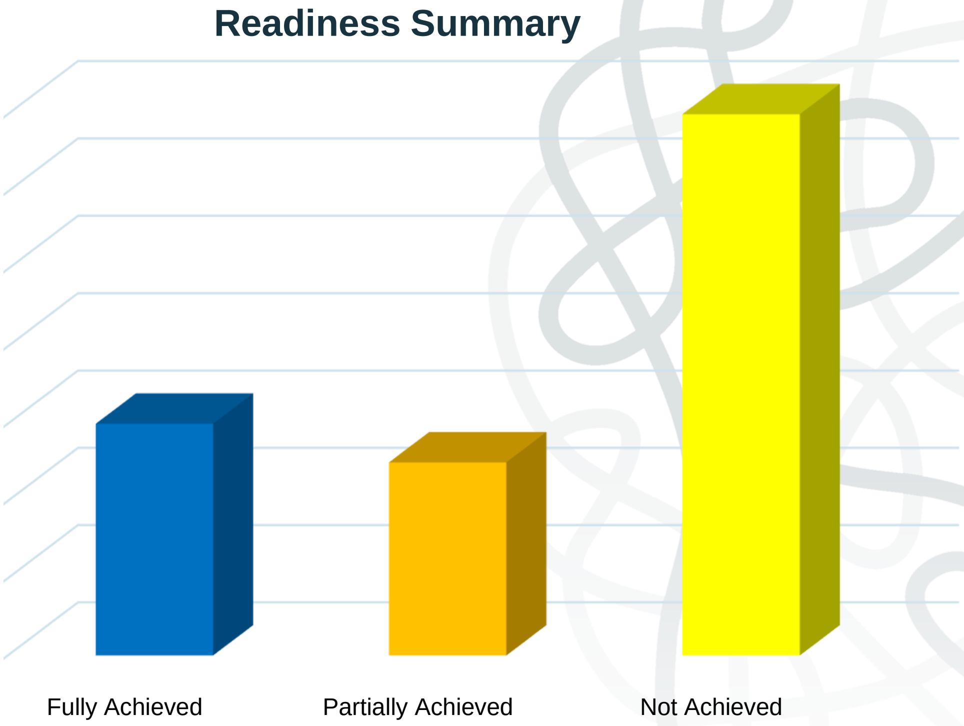
- Risk identification & Treatment
- Policies and procedures
- Change control management
- Incident response
- Contingency planning
- Supplier management
- Assurance testing

Technology

- Asset & Configuration management
- Monitoring & detection

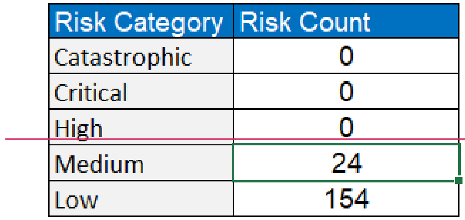
NIS Readiness- Areas for Improvement

- Requirement to align with a recognised cybersecurity risk management forum
- Requirement to formalize cybersecurity governance
- Cybersecurity risk oversight and reporting
- Implement a cybersecurity risk assessment methodology
- Implement formal policies and procedures
- Formalise incident response measures
- Mature business continuity management & DR
- Manage third party security risk
- Implement cyber assurance testing
- Implement an internal audit function



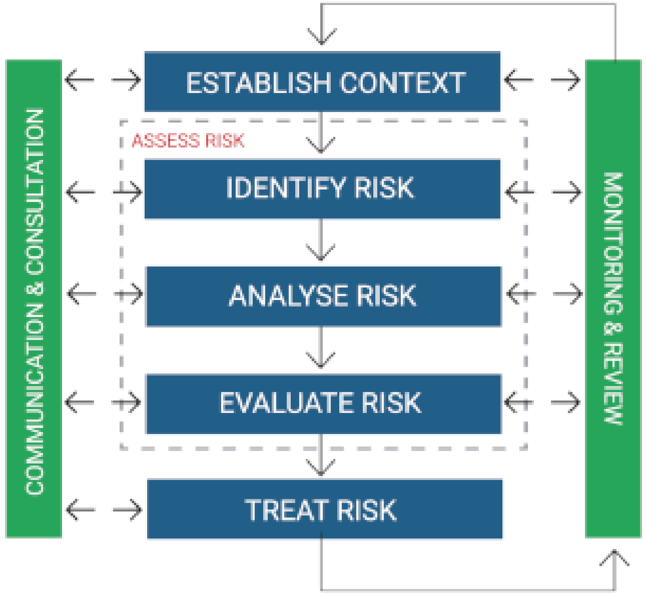
Stage 2- Risk Assessment

Or in a nutshell- Identifying what needs to be done!



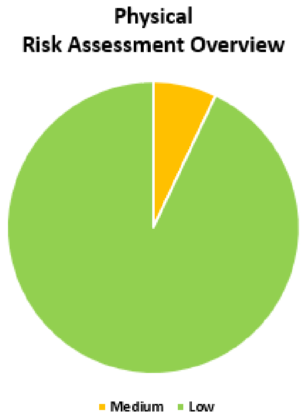
Risk Category	Risk Count
Catastrophic	0
Critical	0
High	0
Medium	24
Low	154

Risk Acceptance

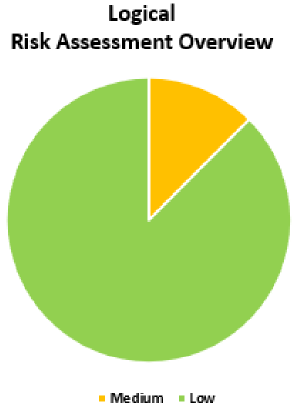


Risk Management Process

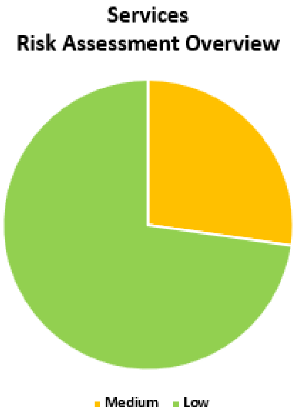
ISO 27005



- People
- Network infrastructure
- End user devices

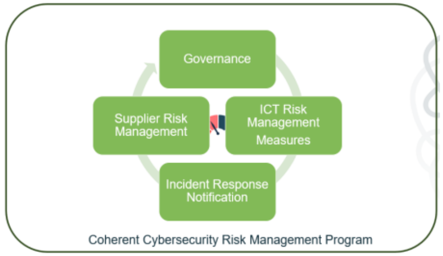


- Network configurations
- Member data
- Employee data
- Data on endpoints
- Web presence



- Data centers
- Dark fiber providers
- Network management
- Security advisory
- Legal
- Financial services

Stage 3- Alignment to ISO27001



Coherent Cybersecurity Risk Management Program

Menu of Security Controls

Mandatory

- Context of the organisation
- Roles & Responsibilities
- Leadership
- Risk assessment methodology
- Performance evaluation
- Improvement

Risk Informed

Organisational Controls

- Competence
- Asset inventory
- Acceptable use
- Lifecycle management
- Access control
- Data classification
- Security in projects management

- Incident management
- BCM
- Supply chain
- Legal and compliance

People Controls

- Screening
- T&C's of employment
- NDA's
- Remote working
- Incident reporting

Technical Controls

- End-user devices
- PAM
- Access to secure code
- Secure authentication
- Capacity management

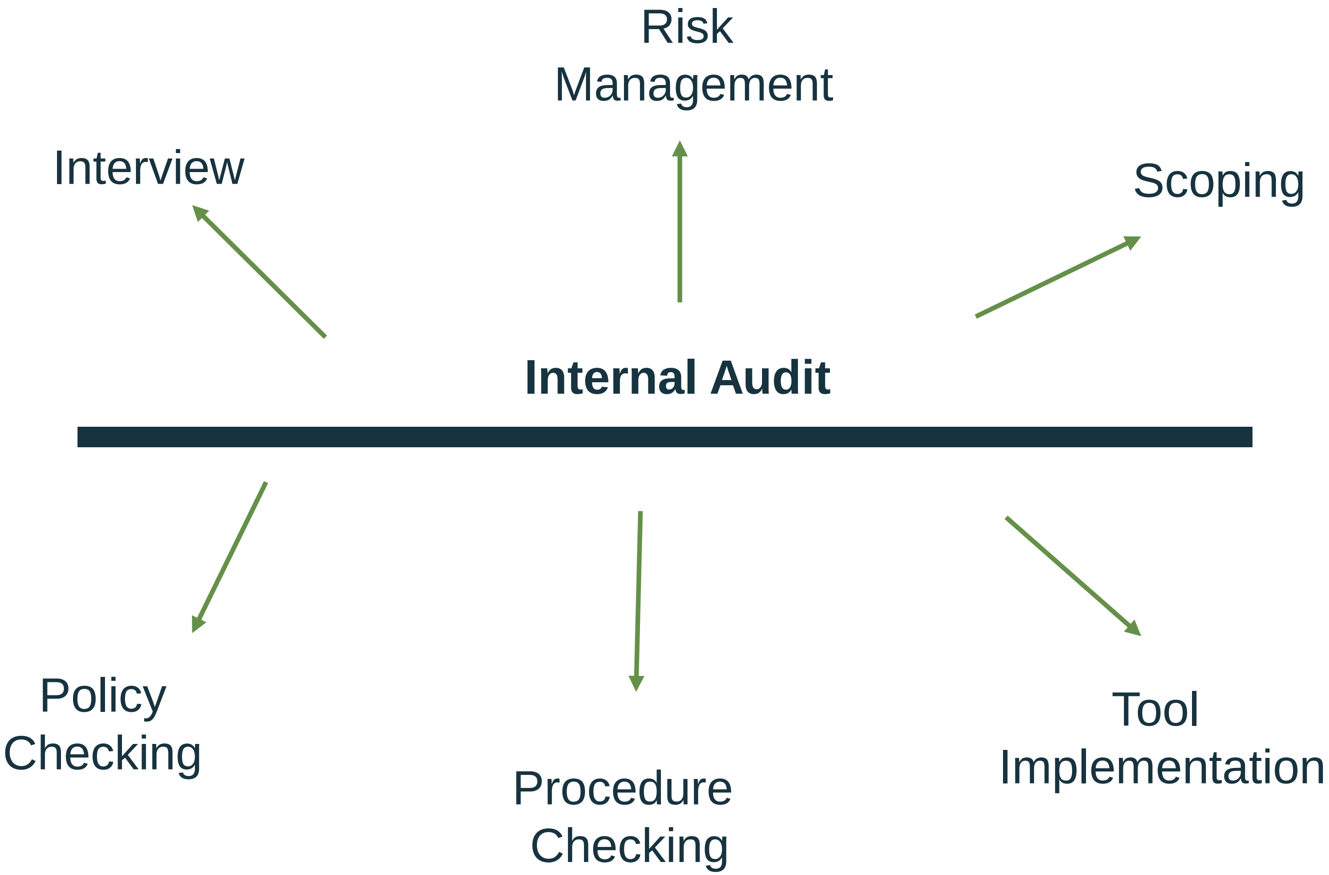
- DLP
- Information backup
- Logging & monitoring
- Threat intelligence
- Cryptography
- Secure coding

- Network security
- Web filtering
- Outsourced development
- Change management

Physical Controls

- Security perimeter
- Entry controls
- Physical security monitoring
- Clear desk
- Supporting utilities
- Equipment disposal

Stage 4- Implementation



Risk Management

Interview

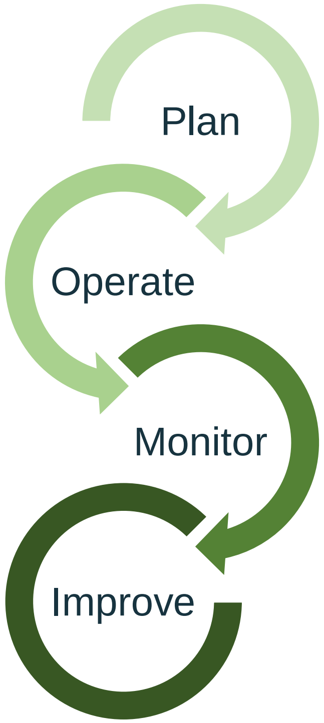
Scoping

Internal Audit

Policy Checking

Procedure Checking

Tool Implementation



Plan

Operate

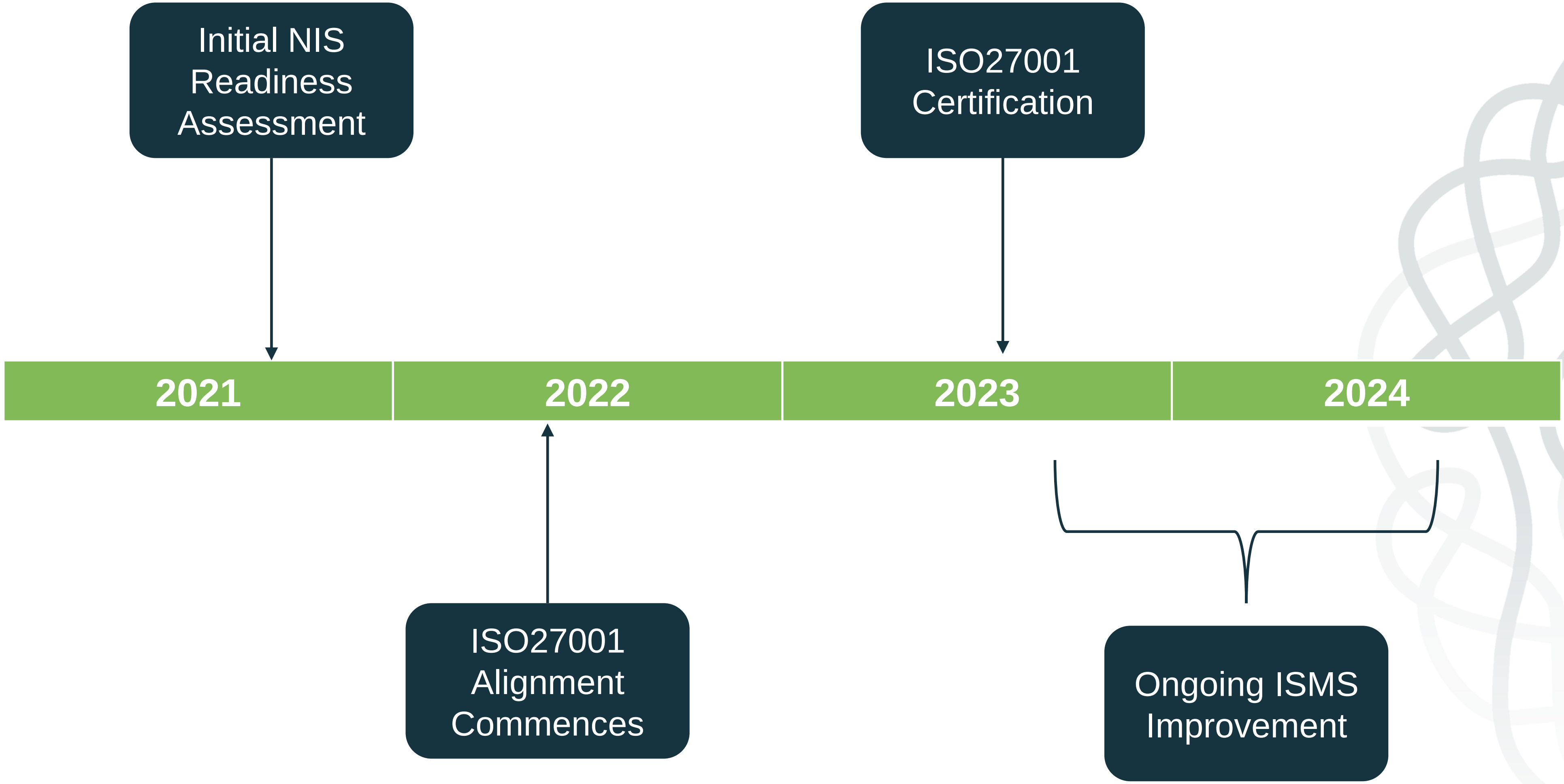
Monitor

Improve

-

Process of Continuous Improvement

Timeline to Certification



Initial NIS Readiness Assessment

ISO27001 Certification

2021

2022

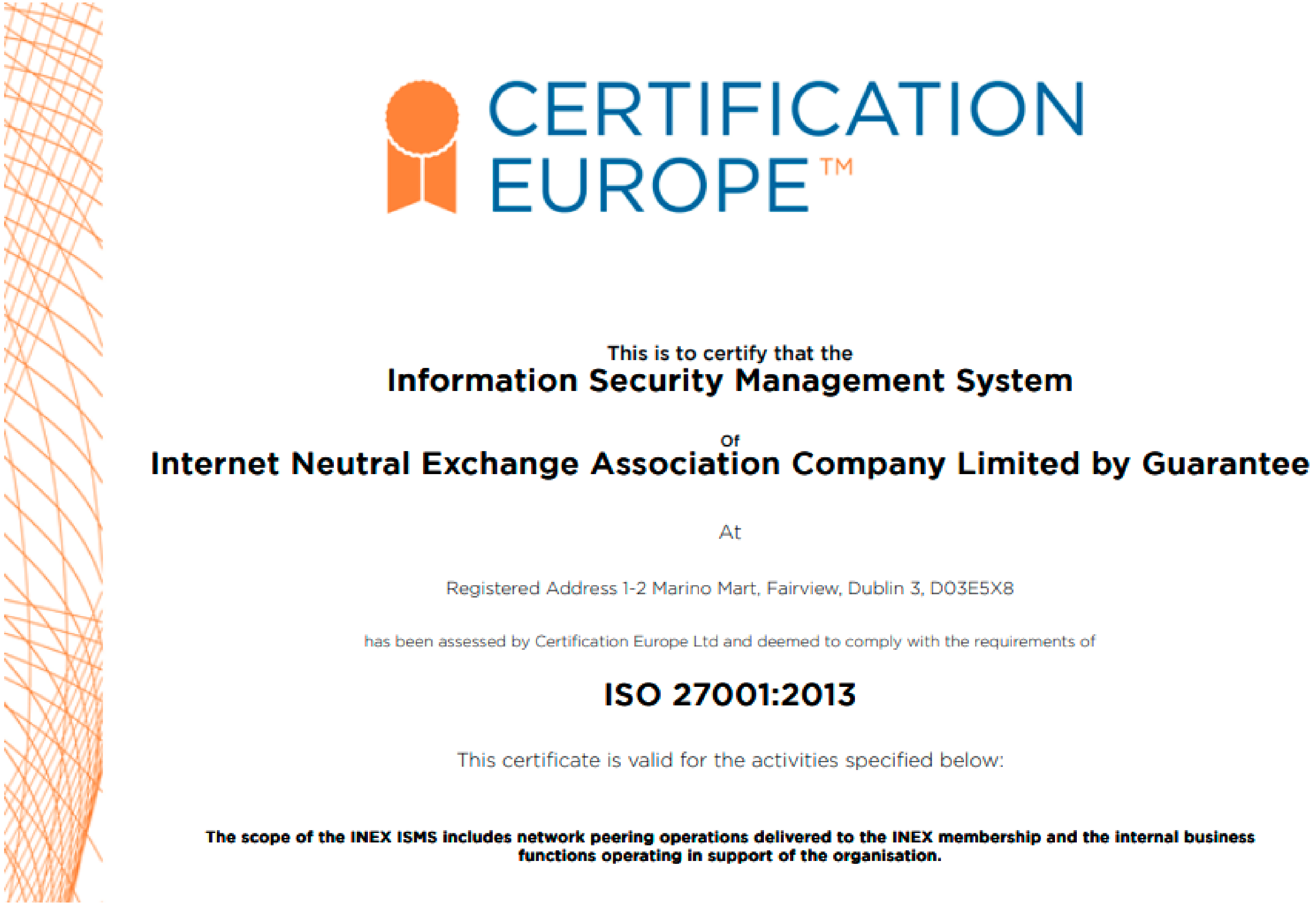
2023

2024

ISO27001 Alignment Commences

Ongoing ISMS Improvement

Achieving Certification



CERTIFICATION EUROPE™

This is to certify that the

Information Security Management System

of

Internet Neutral Exchange Association Company Limited by Guarantee

At

Registered Address 1-2 Marino Mart, Fairview, Dublin 3, D03E5X8

has been assessed by Certification Europe Ltd and deemed to comply with the requirements of

ISO 27001:2013

This certificate is valid for the activities specified below:

The scope of the INEX ISMS includes network peering operations delivered to the INEX membership and the internal business functions operating in support of the organisation.

Lessons from the Journey

Key Consideration #1: Proportionality

- NIS 2: take **appropriate and proportionate** … measures … due account shall be taken of the degree of the entity’s exposure to risks, **the entity’s size** and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

- ISO 27001: proportionality incorporated via risk-based approach and entity’s risk appetite.

Key Consideration #2: Scope

“network peering operations delivered to the INEX membership and internal business functions operating in support of the organisation”

- **BUT** change management explicitly excludes:
  - Changes to internal IT systems.
  - Adding / removing / changing a port or service to members.
  - Changes in test and non-production environments.
  - Changes to third-party services where controlled by the third-party

Benefit #1 – Mature Through Gap Analysis

- Two attitudes to being audited:
  - Fear - hide the gaps, exaggerate, obfuscate, bury legacy
  - Open – full disclosure and open discussion

- Ultimately, culture determines this
  - Requires open, honest, no-fault buy-in from top to bottom

- A true and honest gap analysis provides a roadmap to ISMS alignment and maturity

Benefit #2 – Formalising the Risk Register

- Every organisation has risks.
- Unrecorded risks can be a big issue:
  - No plan to manage those events when they occur
  - No future-looking strategy to mitigate them
  - Can be (ab)used for ‘political’ purposes
- Formalising the risk register addresses these
  - Must be a no-fault / no-blame process
  - Structured was to bring risks into the open - many methodologies
    - ISO 30001 - Risk management
    - ISO 27005 – Application of ISO 30001 to information security
    - 4T’s – threat, tolerate, transfer, terminate
- Primary output: the Risk Register

Benefit #3 – Continuous Improvement

- ISO 27001 10.1: The organization shall **continually improve** the suitability, adequacy and effectiveness of the ISMS.
- ISO audits require evidence: Improvement Register
- Reviewed at every SecCom meeting and minuted

- Becomes a living document.
- Creates an environment where improvement possibilities are identified in day-to-day tasks and added to the register.

- Resourcing is key – “Information Security Manager” is not easy.

Other Benefits

- Policy can be constraining **but** it can also protect.
  - Removes ad hoc ‘workarounds’ to problems
  - Temporary solutions are no longer permanent (audits!)
  - “Policy says ‘no’”
- Formally considers the legal and regulatory systems
- Implementing an ISMS costs money – management buy-in
- Provides comfort to customers and suppliers; additional sales?
- Sharing what we have learned with Members

Thank you

INEX

INTERCONNECTING NETWORKS
AND PEOPLE FOR OVER 25 YEARS