Konfydence
*Outsmart Scams - Together*

# NIS2 / ISO Alignment Brief

## Supporting Human-Risk Awareness under NIS2 & ISO/IEC 27001

### Purpose

This document explains how CoMaSi supports organizations in addressing **human-related cyber risk** through structured awareness and behavior-based learning. It does **not** claim certification or compliance.

### Regulatory context

**NIS2 Directive: Article 21(2)(g)** requires organizations to implement *appropriate and proportionate measures*, including security awareness and training

The directive does not mandate specific tools — it expects **reasonable effort**, relevance, and documentation.

**ISO/IEC 27001:2022**

**Annex A.6.3 – Awareness, education and training** requires that:

- personnel are aware of security risks
- training is relevant to roles
- awareness is reinforced over time

### How CoMaSi supports these expectations

| Regulatory expectation | How CoMaSi supports |
|---|---|
| Awareness exists | Structured scenario-based sessions |
| Training is relevant | Realistic, role-agnostic human-risk scenarios |
| Repeatable | Sessions can be run regularly |
| Evidence available | Behavioral Evidence Template |
| Continuous improvement | Discussion outcomes inform follow-ups |

### Evidence produced (examples)

- Scenario coverage documentation
- Group-level decision patterns
- Discussion notes & learning outcomes
- Follow-up actions (if applicable)

Konfydence

*Outsmart Scams - Together*

**Important disclaimer:** CoMaSi **supports** awareness and risk management efforts. It does **not** certify compliance, replace audits, or provide legal interpretation.