Master NIS2's Human Factor Challenge

The Challenge:

NIS2 mandates cybersecurity awareness training and human risk management, but most solutions focus on compliance theater rather than measurable risk reduction.

Our Solution:

Transform mandatory training into a strategic security capability that satisfies regulators while actually reducing human-caused incidents.

NIS2

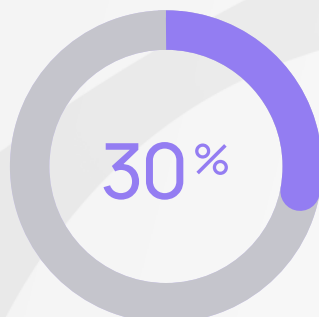
The Human Factor Reality

Core Requirement

NIS2's security framework includes multiple measures where human factors are critical - from awareness training to incident response capabilities.
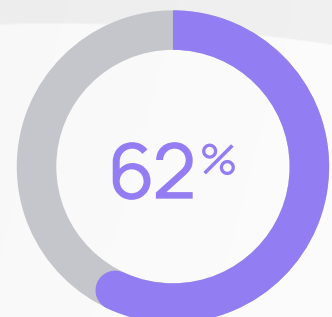
Training Scope

NIS2 mandates extend beyond IT teams - all employees AND management must receive cybersecurity training.

Top Challenge

30%

of IT leaders cite cyber hygiene & awareness as their biggest NIS2 implementation challenge.

Significant Changes

62%

of organizations report NIS2 requirements differ significantly from their current security practices.

How SoSafe Addresses NIS2's Human Risk Requirements

NIS2 Human Factor Requirements	What This Means	SoSafe's Solution
Cybersecurity training	Management bodies must take training; ensure all staff receive regular cyber hygiene education	• Dedicated executive modules with completion tracking • Continuous micro-learning (< 10 min/month) for all staff • 30+ languages meeting native language requirements
Cyber hygiene practices	Adopt practices and raise awareness of phishing, social engineering threats	• Behavioral conditioning via realistic phishing simulations • Real-time threat alerts through Sofie AI chatbot • Policy acknowledgement and acceptance via Sofie AI chatbot
Dynamic risk analysis	Companies must provide risk analysis considering human factors	• Human Risk OS dashboard tracking knowledge, behavior & culture • Automated risk scoring integrated with technical security data • Predictive analytics to prevent incidents before they occur
24-hour incident reporting	Report significant incidents within 24 hours of awareness	• Phishing Report Button for instant user reporting • Threat Inbox automated triage • Integration with incident management systems

ROI Beyond Compliance

Incident reduction	**5x** lower social engineering risk within 12 months
Faster reporting	**60%** of employees become threat sensors
Insurance benefits	Reduced cyber insurance premiums with demonstrated human risk management
Transferable compliance	One program satisfies NIS2, DORA, ISO 27001 human factor requirements

Trusted by 5,500 customers in regulated industries across Europe

> " While compliance is crucial, our focus goes beyond just ticking the boxes. SoSafe, with its ISO Reporting Tool, not only helps us meet compliance requirements but also allows us to manage real risks, secure customer data, and foster a security culture that mitigates human risk—something far more impactful than simply passing audits.
>
> Roald Roos, CISO at Fellowmind

> " In the midst of the regulated critical infrastructure sector, we face significant challenges, from implementing the NIS2 Implementation Act to adapting to the EU CER regulation. Together with the other infrastructure companies in the 21 Group in Dortmund, we were looking for solutions to overcome these challenges and build a robust online future in this regulated sector that we are in.
>
> Jens Feistel, CISO DEW21

Start Your
Human Factor
Compliance Journey

Don't wait for final regulations — build your human firewall now.

Compliance Alignment Statement
Compliance Note: While SoSafe addresses key human risk components of NIS2, comprehensive compliance requires technical and governance controls beyond our platform. National implementations may vary—consult your legal team for specific requirements.