



NIS2 Guide: Roadmap to meeting security training obligations

Practical steps, realistic timelines, and audit-readiness



Overview

Executive summary	3
Navigating NIS2: authorities, entities and timelines	4
National transpositions of NIS2 and emerging differences	6
NIS2's baseline requirements organisations cannot overlook	8
Securing organisations through their people	10
Factors to consider when choosing a training and awareness solution	13
SoSafe solutions mapped to regulatory demands	14
Fast-track to awareness compliance in 90 days	17
Take the next step toward readiness	18

Executive summary

The pandemic showed how quickly digital systems can falter and how vulnerable critical services can be. Europe responded with [NIS2](#), **a stronger directive** that replaces the 2016 one, aiming for clearer accountability and greater resilience.

The new directive widens its scope to **cover more sectors**, and it lands just in time. In the past year, nine out of ten organisations experienced a cyber incident of **the kind NIS2 is meant to prevent**, and almost half were hit more than once, according to a [2024 survey](#). Those numbers show just how overdue stronger rules had become.

That is the context NIS2 steps into: pushing accountability higher, widening its scope, and demanding proof of resilience. Yet 53% of IT leaders still question whether [NIS2 is adequate](#). Its requirement, however, is simple: show that you are prepared.

Today, NIS2 is set to affect more than **180,000 organisations across Europe**, from healthcare and transport to manufacturing and the wider supply chain. SoSafe has long supported these sectors in the area of cybersecurity now under scrutiny: **awareness and training**. [30% percent of IT leaders](#) say this is the **toughest aspect of NIS2** compliance, although in practice the difficulty often lies in how it is tackled.

NIS2 does not ask if training exists. It asks if it works, if it reaches the right people, and if it can be proven.

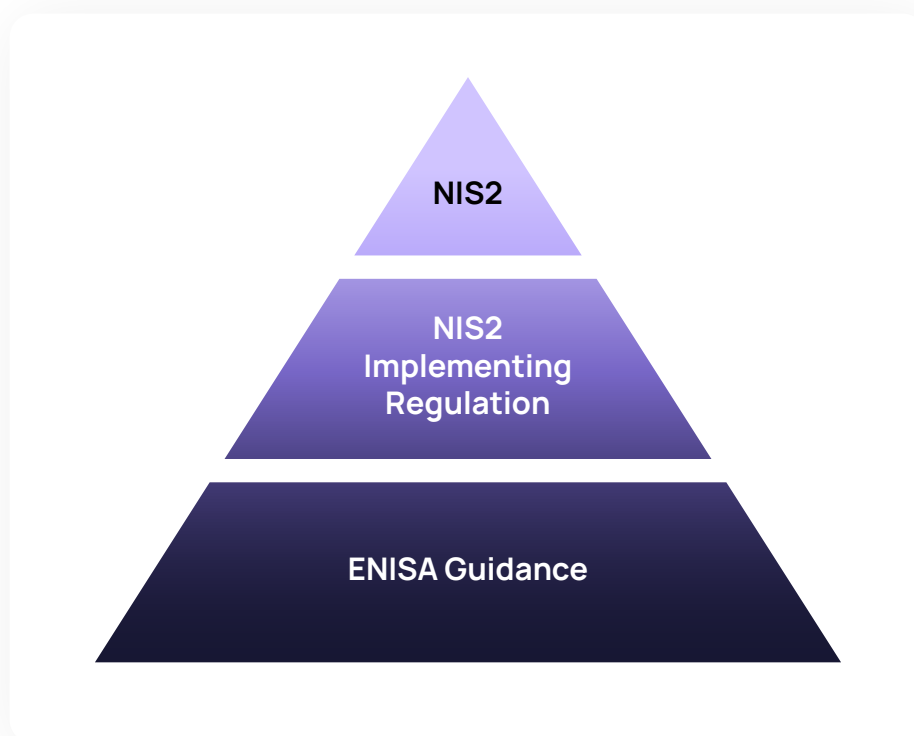
SoSafe helps organisations meet that standard with programmes built for compliance but designed to change behaviour from within.

This guide sets out what NIS2 expects of organisations in building a security culture and shows how to **prepare with evidence** that earns regulator confidence and builds trust.

Navigating NIS2: authorities, entities and timelines

Behind NIS2 is a framework that combines clear rules with practical support, giving organisations both obligations to meet and systems to rely on.

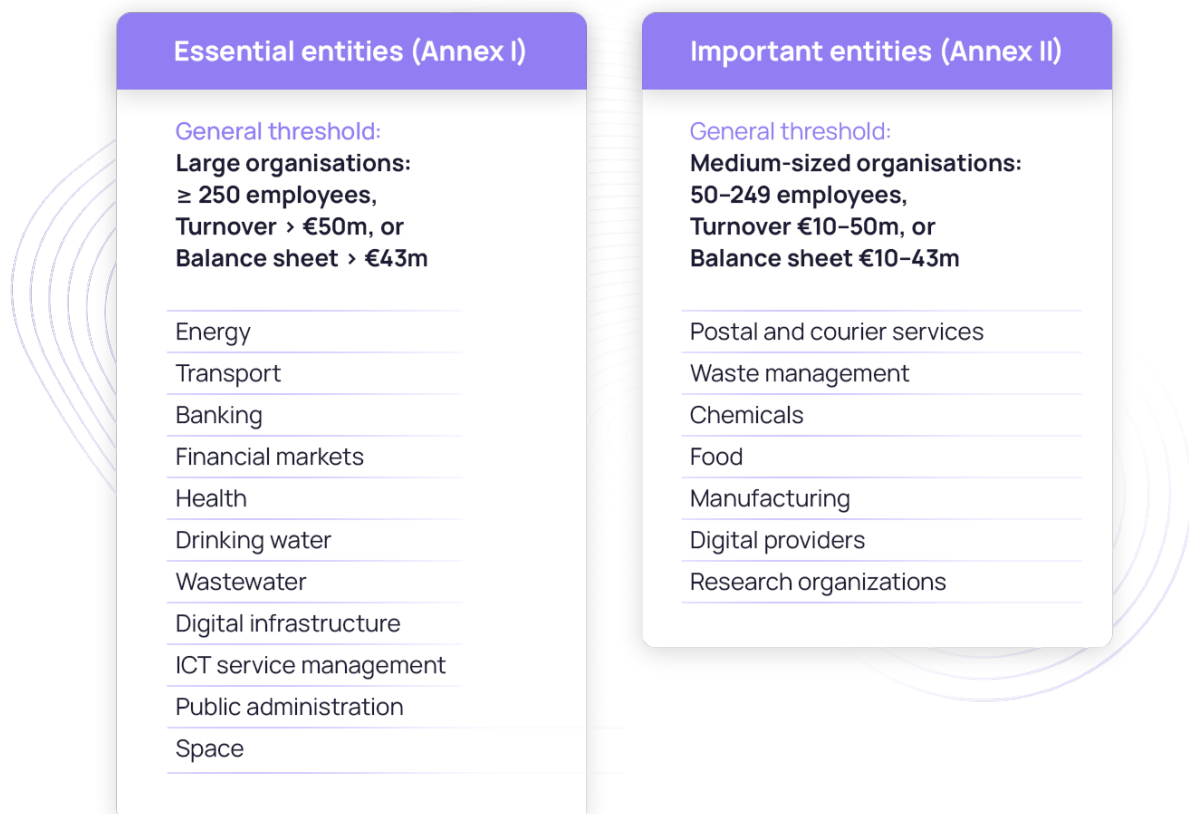
The **rulebook has three layers**: the [directive](#) sets the rules, the [regulation](#) makes them specific for digital sectors, and ENISA's [guidance](#) shows how to apply them. Other sectors can use the guidance as good practice, but national rules take priority.



Alongside this, NIS2 creates a **coordinated defence system** organisations can turn to when incidents escalate. National CSIRTs provide frontline response, while EU-CyCLONe and the NIS Cooperation Group handle cross-border coordination and shared guidance. NIS2 also introduces an EU-wide [vulnerability database](#) so organisations can [register](#) them early.

NIS2 mainly applies to **medium and large organisations in critical sectors**. Micro and small firms are excluded, unless a Member State decides otherwise. Some entities – like trust service providers, DNS/TLD registries and central administrations – are always in scope regardless of size.

Cross-border companies answer to their main EU base instead of multiple national authorities, but subsidiaries can still be included since **thresholds apply at group level**. Each Member State must keep a list of essential and important entities, and companies need to check their status nationally.

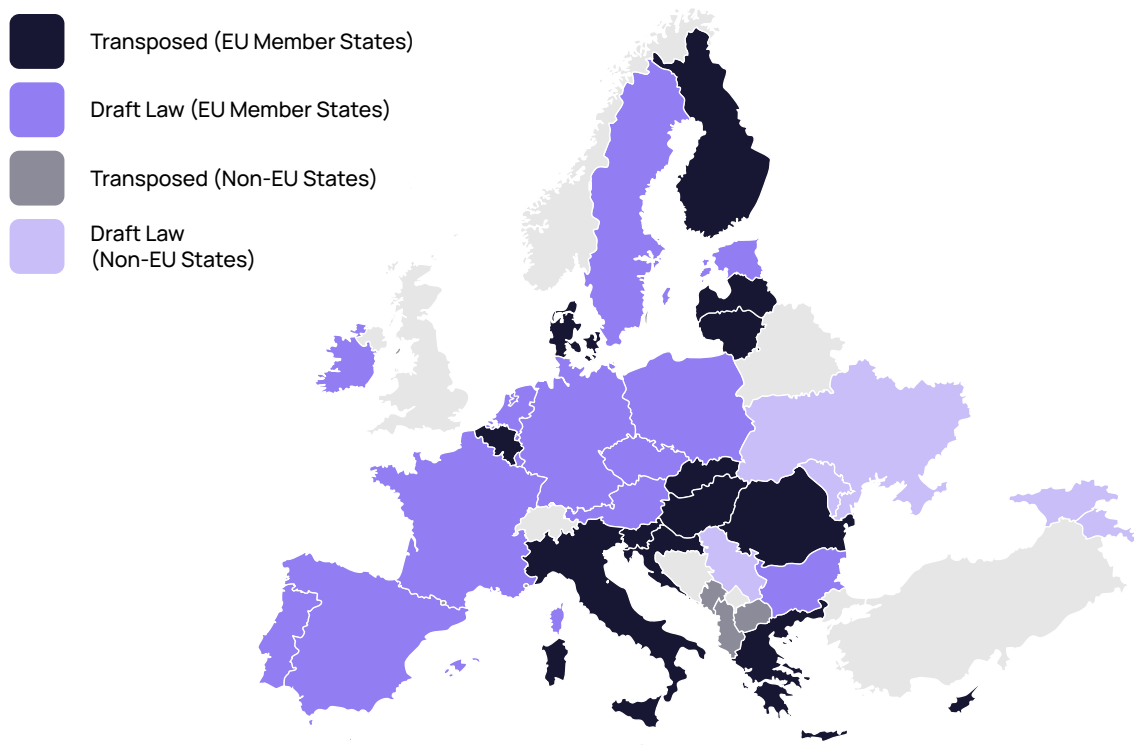


Companies in scope should expect closer oversight. Authorities can carry out **audits and inspections**, demand corrective measures, and impose penalties. **Fines can be steep**, and reach up to €10 million or 2% of global turnover for essential entities, and €7 million or 1.4% for important ones.

Transposition deadlines are fixed at EU level, but **national progress varies**, making it vital for organisations to follow local developments. With enforcement close behind, organisations have no time to lose.

National transpositions of NIS2 and emerging differences

By August 2025, only **14 of 27 Member States** had [transposed NIS2](#), prompting the Commission to open infringement cases the previous November.



Source: [European Cyber Security Organisation \(ECSO\)](#)

ECSO highlights the areas where differences are most pronounced.

Scope and sectors	<ul style="list-style-type: none">• Hungary, Finland and Belgium excluded banking and finance (already covered by DORA).• Spain added nuclear, while Poland moved manufacturing into the “essential” category.• Several countries, including Hungary, Slovakia and Germany, merged drinking water and wastewater into a single sector.
Frameworks	<ul style="list-style-type: none">• Some countries specify ISO 27001/27002 (Croatia, Finland, Slovenia), others use NIST 800-53 (Cyprus) or NIST CSF 2.0 (Ireland).• Belgium, Romania and Lithuania adopted tailored national frameworks, while Greece, Hungary, Latvia and Slovakia refer vaguely to “international standards.”
Reporting	<ul style="list-style-type: none">• Cyprus requires alerts within six hours. Slovakia goes further, demanding reports of prevented threats and unmitigated vulnerabilities.• Malta starts obligations nine months after classification; Czechia a year after registration.• Greece sets different deadlines depending on entity type.
Registration	<p>Company registration deadlines also vary: one month after entry into force in Romania, three months in Austria, and early 2025 dates across Ireland and Sweden (January), Italy (February) and Denmark (April).</p>
Enforcement	<ul style="list-style-type: none">• Hungary mandates bi-annual audits by certified external auditors.• Romania requires annual self-assessments with 30-day corrective plans.• Belgium and Croatia introduced tiered penalties, while Luxembourg applies GDPR-style fines for budgetary bodies.

Where rules differ across borders, **many companies choose to follow the strictest national standard** and record justified deviations.

With transposition underway, the spotlight now shifts to the substance of NIS2 itself: the controls it sets, the governance it demands, the evidence it requires, and the way incidents must be reported.

NIS2's baseline requirements organisations cannot overlook

National transpositions may differ, but the obligations are the same across Europe. Organisations are expected to put **proportionate**, state-of-the-art controls in place, prove they work, and address vulnerabilities without delay (Art. 21).

To create a level playing field, NIS2 sets out **10 essential elements** that every organisation must embed in practice.

Core NIS2 requirements (Art. 21(2))

1. Risk analysis and security policy.
2. Incident handling.
3. Business continuity and crisis management (backups, recovery).
4. Supply-chain security for direct suppliers and service providers.
5. Secure acquisition, development and maintenance (with vulnerability handling and disclosure).
6. Effectiveness testing of measures.
7. Basic cyber hygiene and regular cybersecurity training.
8. Cryptography and encryption where appropriate.
9. HR security, access control and asset management.
10. Strong authentication and secure communications.

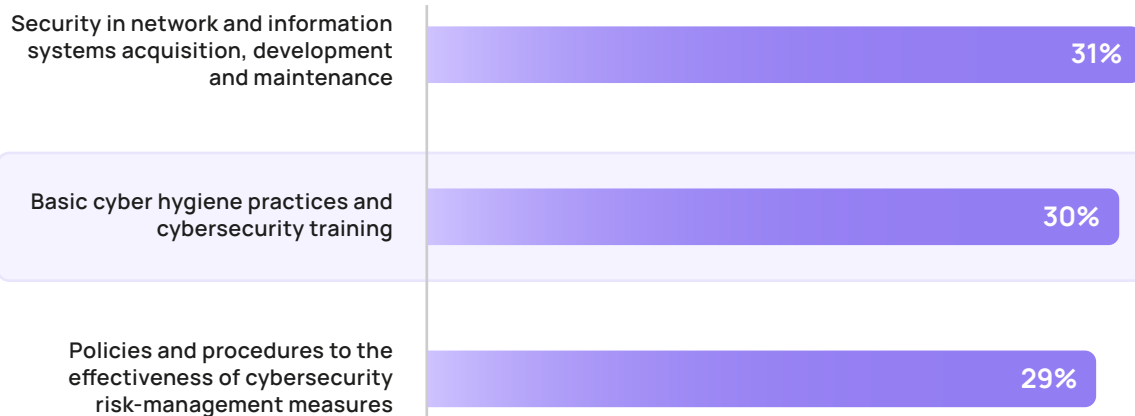
Incident reporting carries the strictest timelines: an early warning within 24 hours, a notification in 72, and a final or progress update within a month. Clear roles, reliable records, and smooth communication are essential to deliver on this (Art. 23).

Responsibility also extends to the **supply chain**. Organisations must assess supplier vulnerabilities and development practices, factoring in EU-level risk assessments.


(Art. 22). The **directive sets the baseline**: governance at the top, resilience across systems and suppliers, and accountability through fast, transparent reporting. It also places clear emphasis on training and awareness.

Together, these requirements are designed to lift cybersecurity to a common standard across Europe. Yet many obligations remain **poorly understood**, turning compliance into a moving target. 3 in 10 IT leaders say [cybersecurity training is the toughest part of NIS2 compliance](#), ranking it the second biggest challenge overall.

Top 3 compliance challenges for IT leaders under NIS2



Source: [Zscaler, 2024](#)



The directive puts the human factor on par with technical controls (Recital 78) and makes awareness a measurable obligation. Employees need **training that reflects real-world threats** like phishing and social engineering (Recital 89). Leadership is not exempt either. **Boards** must oversee the programme, complete training themselves, and accept personal accountability for failures to comply (Art. 20).

"Article 20(2). Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity."

The directive codifies technical standards, but it also recognises that people, their judgment, their training and their accountability remain decisive.

Securing organisations through their people

The human factor has always played a role in cybersecurity risk. In 2024, nearly [seven in ten](#) breaches (68%) involved some element of human error. Security leaders recognise the pattern: four in ten believe their next major incident will start with a [human vulnerability](#). Concern is even higher in Spain (53%), France (45%) and the DACH region (44%).

Attackers understand this too. They don't need to force entry when persuasion works just as well. Authority, urgency and misplaced trust are their favourite levers. In a moment of stress or distraction, even well-trained employees can be caught off guard.



Breaches now cost millions – an average of [€4.4 million](#) each, with sectors like healthcare facing even greater losses. Regulators see the same trend, which is why awareness and training are now written into law.

Compliance looks different as a result. Attendance sheets and tick-box courses no longer suffice. Regulators expect visible signs of behaviour change.

NIS2 makes awareness and hygiene part of compliance itself, with ENISA reporting on progress every two years (Art. 18). Its [guidance](#) turns broad rules into practical steps organisations can act on and prove, as the example below shows.

"8.1.2. For the purpose of point 8.1.1., the relevant entities shall offer to all employees, including members of management bodies, as well as to direct suppliers and service providers where appropriate in accordance with point 5.1.4, an awareness raising programme, which shall:

- (a) be scheduled over time, so that the activities are repeated and cover new employees;
- (b) be established in line with the network and information security policy, topic-specific policies and relevant procedures on network and information security;
- (c) cover cybersecurity risk-management measures in place, contact points and resources for additional information and advice on cybersecurity matters, as well as cyber hygiene practices for users."

Source: [ENISA](#)

In effect, the directive treats people as a security risk that can be managed. The documentation shows how:

Awareness for all	Recurring programmes for staff, management, and where relevant, suppliers, aligned with security policies.
Role-specific training	Targeted, practical training for admins, developers, and other high-risk roles, with certifications where needed.
Core hygiene	Strong authentication, phishing and social engineering awareness, safe browsing, backups, updates, and secure remote work.
Testing and updates	Quizzes, exercises, or feedback to measure impact, with annual refreshes to keep pace with evolving threats.
Tracking and evidence	Logs, metrics, certificates, and attendance records to demonstrate compliance and prove completion.

Taken together, these steps show what compliance looks like in practice. But it is also where many organisations stumble.

Designing, delivering, and evidencing **programmes at scale** takes structure, expertise, and reliable data. Without that, compliance is out of reach, and so is resilience against attacks that still most often start with people. A trusted partner can close the gap, providing both the capacity and the proof regulators now expect.

Factors to consider when choosing a training and awareness solution

If you are exploring external support, choosing well is important. Compliance takes time and budget, and the return depends on the partner you select. The following questions can guide your decision.

Key questions to ask vendors on NIS2 human risk compliance:

- ☐ Is the training available in **every language** your staff needs, and **continuous** so new hires are always covered?
- ☐ Can **non-desk (or field) staff** access training too? Are options like in-person sessions, print materials, or shared devices available?
- ☐ How are **incidents** from users formally escalated?
- ☐ Can the provider give evidence in **auditor-recognised formats**, like ISO, and export it easily?
- ☐ Can the tool deliver training through **channels employees already use**?
- ☐ Where is your **data** stored, what laws apply, and how long is it retained?
- ☐ Which **enterprise integrations**, such as Teams, Outlook, Entra ID or LMS/LXP, are supported natively and how are they maintained?
- ☐ Can training be **tailored to roles, functions and risk-profiles** in your organisation?
- ☐ How is training **effectiveness** assessed in practice, and which **behavioural metrics** are tracked over time (e.g. click rates, reporting rates, high-risk groups)?
- ☐ What ensures training and reporting **evolve** with changing risks and laws?

SoSafe solutions mapped to regulatory demands

Across Europe, most companies already run cybersecurity training, but much of it is outdated, one-size-fits-all, and leaves no proof it actually works. NIS2 makes that no longer acceptable. Regulators want evidence that staff across the organisation, from executives to non-desk employees, are trained in ways that fit their roles, that behaviour improves over time, and that results can withstand an audit. For most teams, this is the point where traditional awareness programmes show their limits. Closing those gaps requires **a system built for compliance and resilience in equal measure**.

SoSafe was designed for that reality. Its programmes **make awareness continuous**, with short sessions in more than 30 languages and dedicated modules for boards and executives.

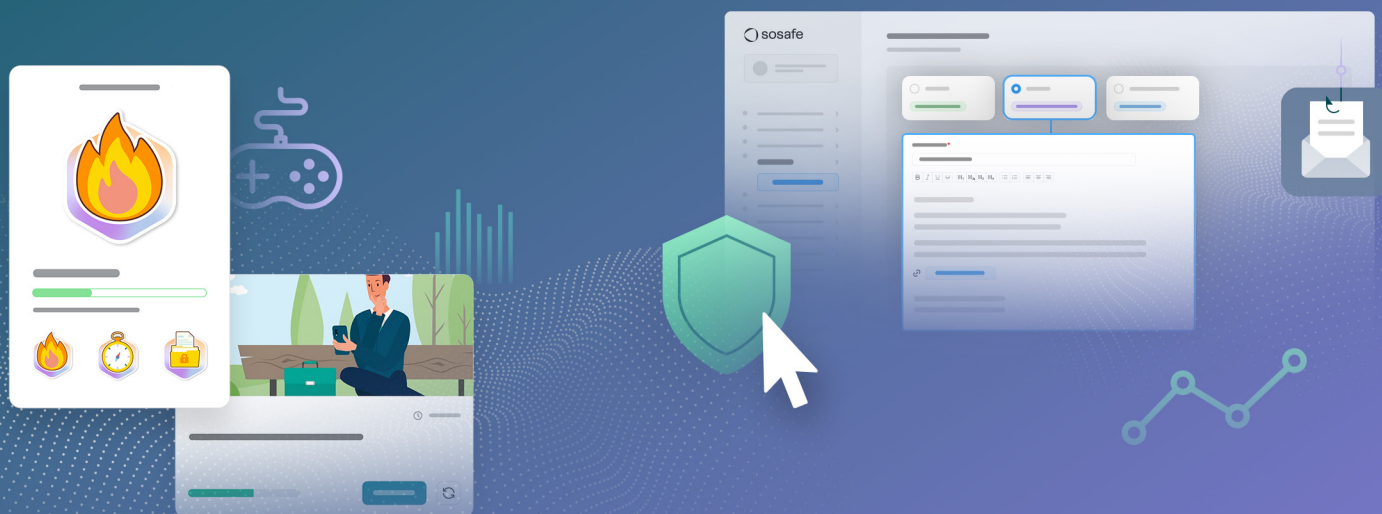
Phishing Simulations tests readiness in real conditions and generates hard data on how people respond, while the **Phishing Report Button** channels incidents straight into security workflows.

Article 20 (2)

Personalised Learning

Article 21(2) (g)

Phishing Simulations



Behind the scenes, the **Human Risk OS** collects analytics across the organisation, combining behavioural insights with technical signals to show not only who has completed training, but whether the organisation is genuinely reducing risk. **ISO and NIS2 compliant reports** are generated automatically, and the data can be exported to third party systems via API, removing the scramble to prepare when regulators come calling.

Article 21(2)(f)

Human Risk OS

What sets SoSafe apart is how **awareness becomes part of the everyday environment**. Instead of sitting outside the flow of work, it is woven into the tools people already use: Teams, Outlook, Slack, Gmail or existing learning platforms.

Sofie, the AI assistant, is on hand to answer questions, flag suspicious emails, and push urgent alerts directly to staff. Policy management and threat reporting live in the same space, so nothing gets overlooked. The result is a **security culture** that is visible, measurable, and practical in daily operations.

Article 21(2)(b)

Phishing Report Button

Article 23(4)(a)

Sofie, AI copilot



And it works. Organisations using SoSafe report **5x lower social engineering risk**, faster reporting as more employees become proactive, and even lower insurance premiums thanks to demonstrated control of human-factor risks.

Independent reviews show that **SoSafe's solutions** not only fulfil NIS2 obligations but also align with **frameworks like ISO 27001, DORA, TISAX, BaFin, and PCI DSS**. For organisations, that means compliance can be demonstrated across multiple standards with one scalable system.

With more than **5,500 customers across Europe**, the platform helps turn one of the hardest parts of compliance into something structured, provable, and sustainable.

Here's how organisations are already using SoSafe to meet NIS2 requirements:

Fellowmind unified fragmented tools across five countries to prepare for NIS2

Fellowmind

The programme included a dedicated **Cyber Security for Managers** track to brief executives on accountability.

Results:

Phishing interactions fell

74%

Simulated click rates dropped to

3.5%

Training scores averaged

97%

ISO reporting toolkit delivered **audit-ready evidence** for NIS2, ISO, and GDPR

DEW21, a regulated energy utility facing both NIS2 and CER obligations, adopted a programme built on steady practice

DEW21

Results:

Phishing click rates fell

54%

in year one

Detection and reporting rose to

43%

Employees rated training

4.9/5

Created a **traceable evidence trail** to meet supervisory expectations.

Fast-track to awareness compliance in 90 days

Use this 90 day path to turn NIS2's human risk obligations into practice and evidence without stalling your operations.

NIS2 Cybersecurity Training Implementation Checklist

Days 1-30: Foundation and leadership

- ☐ Brief management body and schedule their training.
- ☐ Segment people into cohorts (management, high-risk teams, general workforce.)
- ☐ Run baseline phishing and knowledge assessments.

Days 31-60: Targeted training and reporting

- ☐ Deploy personalised training for employees.
- ☐ Deploy role-based modules for high-risk teams, non-desk staff and managers.
- ☐ Introduce Sofie (AI chatbot) integration with Teams or Slack.
- ☐ Switch on phishing simulations.
- ☐ Implement reporting tools and train staff on procedures.
- ☐ Update board and brief key suppliers.

Days 61-90: Full deployment and compliance

- ☐ Compile evidence pack with training records, initial test results, and reporting logs.
- ☐ Set clear targets for completion, click rates, and reporting rates.
- ☐ Run internal audit dry-run and fix gaps.

Ninety days in, security will be part of the routine: leaders are more engaged, staff is being trained, suppliers are aligned, and the evidence is in place. Keep the cycle going and awareness stays sharp while results improve and audits become manageable.

Take the next step toward readiness

Modern security teams face three pressures at once: employees with little time, attackers who constantly adapt and auditors who demand evidence. NIS2 requires organisations to meet all three by embedding security into everyday work. This is an operating model that strengthens over time. And its payoff is exactly what matters most: fewer incidents, proven compliance and a stronger security culture.

SoSafe's experts help design that model with you, build it into the tools your people already use and generate evidence that stands up to scrutiny. Reach out to arrange a readiness session and leave with a tailored plan you can execute immediately.

Let's talk