



Business Track

NIS2: the day after



Koen Tamsyn



**Business Unit Lead
Cybersecurity | CISSP**



Koen.tamsyn@inetum-realdolmen.world

02 801 53 97

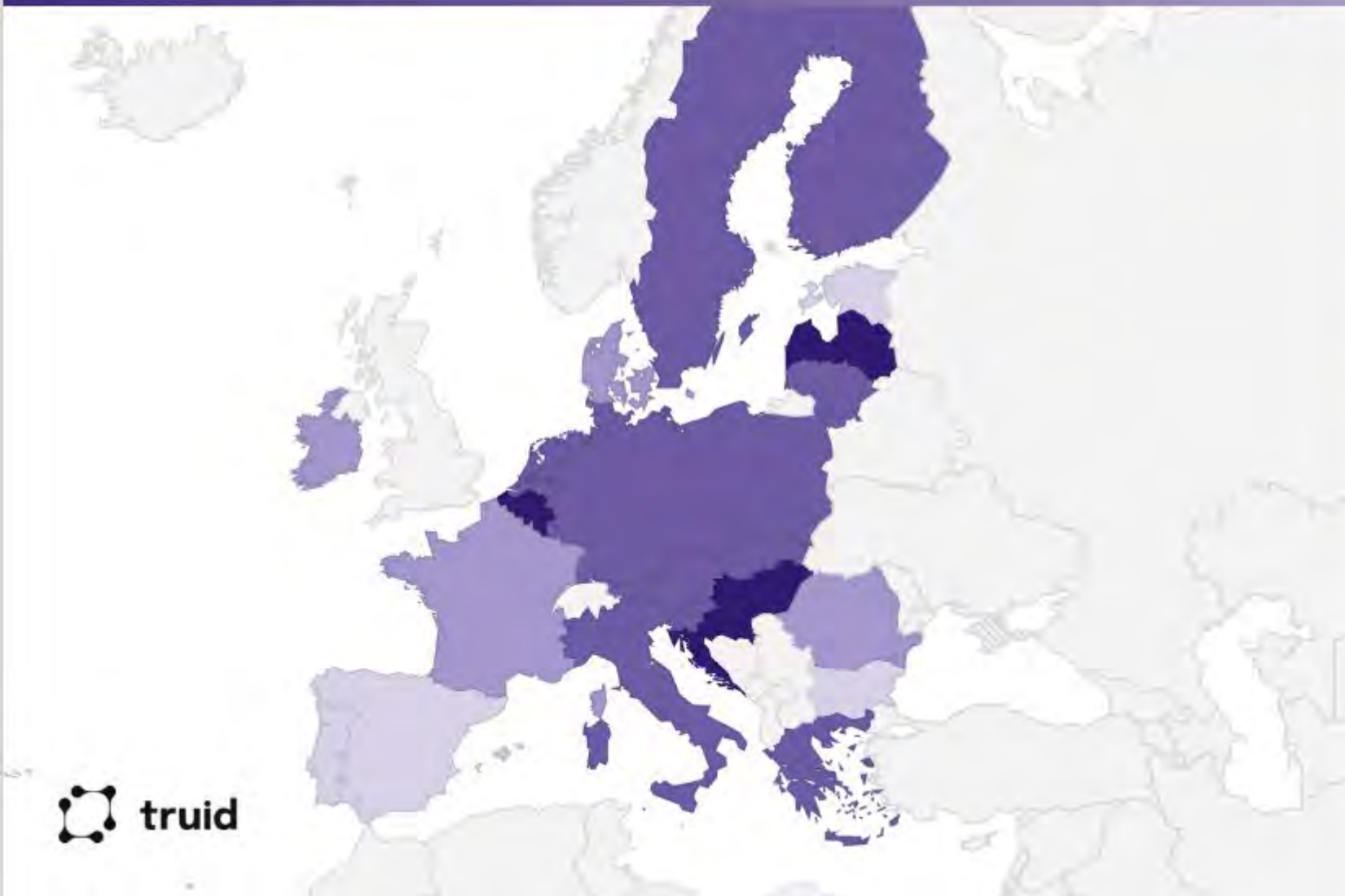


**NIS2 Directive Transposition Deadline
for the Member States: October 17, 2024**

A cinematic, post-apocalyptic scene of a city street. The street is overgrown with green weeds and grass. In the foreground, a rusted, abandoned car is parked on the left. To the right, there is a pile of debris, including a crushed car. The street is wet and reflective. In the background, tall, modern skyscrapers rise against a cloudy sky. The overall mood is desolate and haunting.

WE WERE NOT PREPARED..

Status of NIS 2 Directive Transposition



- Stage 4**
Transposition of NIS 2 directive into national law
- Stage 3**
Draft has been submitted, waiting for feedback or approval
- Stage 2**
Initial stages of development announced and some progress made
- Stage 1**
Limited information available or minimal progress made

NIS2 Timeline

Essential entities

18 October

2024

Registration

After 18 October 2024, organizations will have 5 months to register with the CCB as an essential or important organization. Entities need to report significant incidents.

18 April

2026

Verification

Entities that have opted for the “Basic” or “Important” assurance level must have their self-assessments verified by an accredited CAB or the CCB.

18 April

2027

Certification

Entities that must comply with the “Essential” assurance level must acquire a certification from an accredited CAB.

** Important entities are not subject to mandatory regular conformity assessments (because of ex-post supervision only)*

NIS2 Timeline

18 October

2024

Registration

After 18 October 2024, organizations will have 5 months to register with the CCB as an essential or important organization. Entities need to report significant incidents.

The NIS2 law & Royal Decree will enter into force on 18 October 2024. Consequently, and subject to exceptions, all obligations of the law and the Royal Decree will apply to essential and important entities from that date (cybersecurity measures, incident reporting, etc.).

By way of exception, regular conformity assessment of essential entities will be introduced gradually and in a differentiated manner, depending on the chosen reference framework

A magnifying glass with a black handle and frame is positioned over a stack of white papers. The background is a soft-focus bokeh of warm, golden-yellow and orange light spots. The text is overlaid in white, sans-serif font across the center of the image.

Inspections of important entities are carried out based on indicators, such as the occurrence of an incident or objective evidence of possible shortcomings.

NIS2 Benefits



Reduced Risk Cyber Incidents

Fewer breaches and attacks reduce financial losses (ransom, downtime, ...)



Improved Stakeholder Trust

Customers and partners prefer companies with strong cybersecurity practices.



Compliance Avoids Penalties

Non-compliance can lead to significant fines and legal consequences.



Enhanced Reputation

Preventing cyber incidents protects your reputation and avoids negative publicity.



Improved Operational Efficiency

Enhanced cybersec measures streamline processes and improve overall performance.



Market Differentiation

NIS2 Compliance offers a competitive edge, especially with regulated entities.



Lower Cybersec Insurance Fees

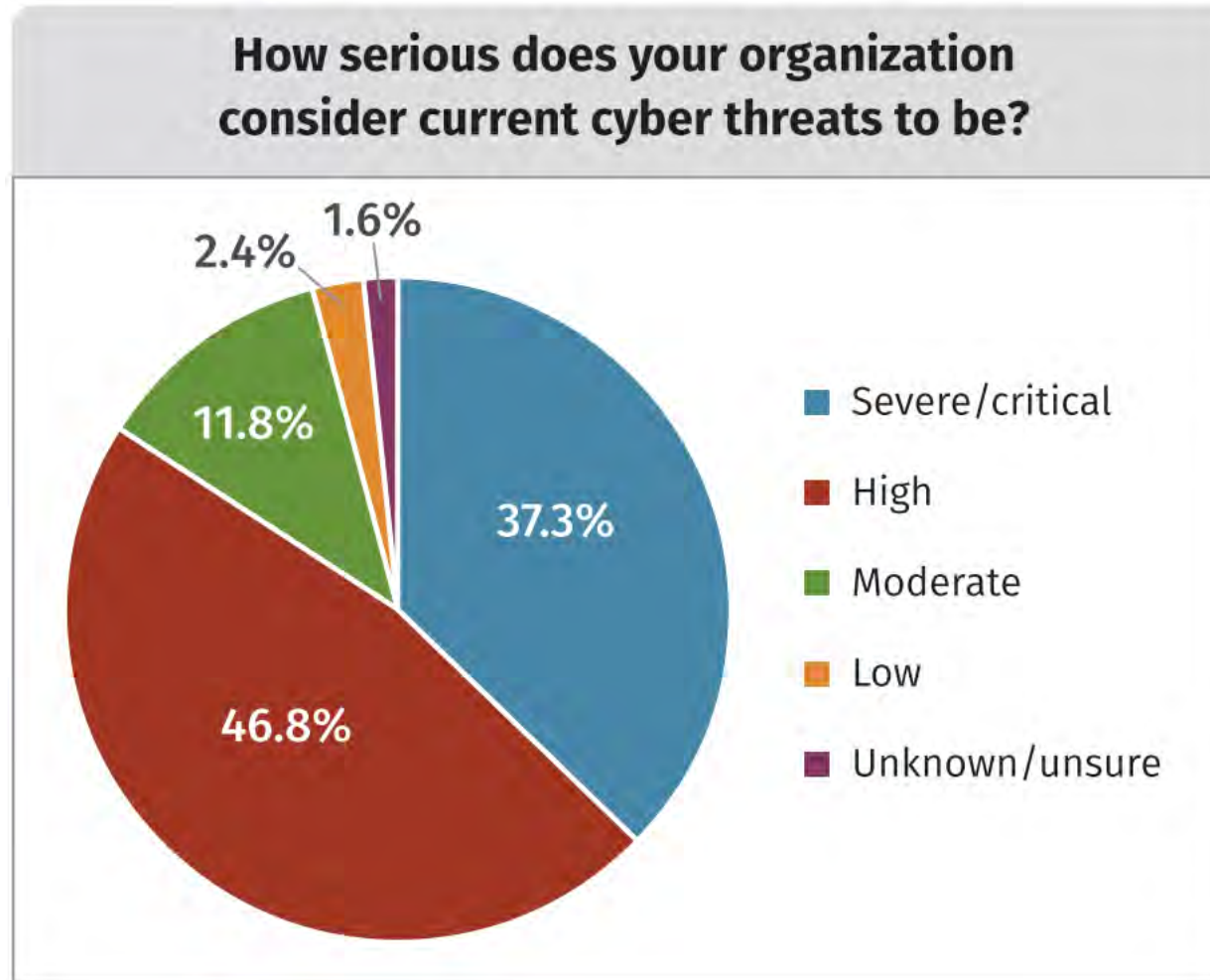
Many insurers offer discounts when demonstrating robust cybersec measures.



Future-Proofing

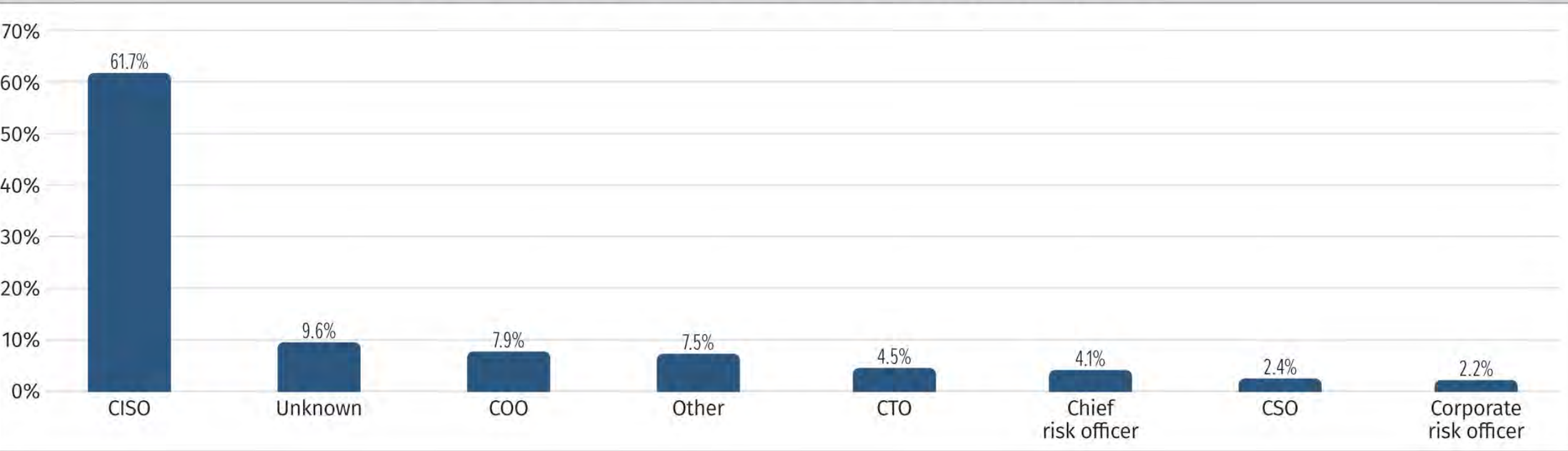
NIS2 alignment ensures readiness for future regulations.

NIS2 and Awareness

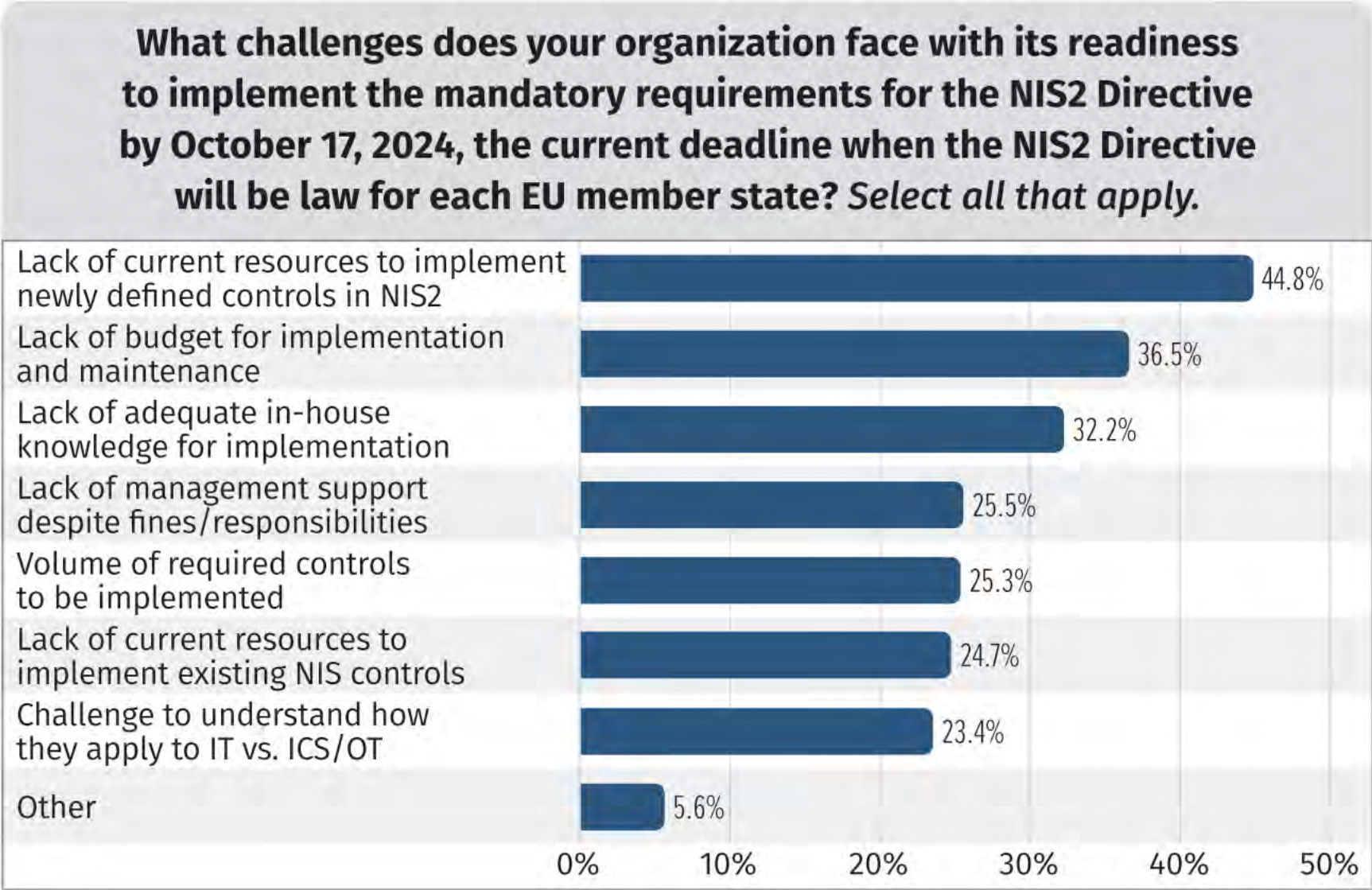


NIS2 and Awareness

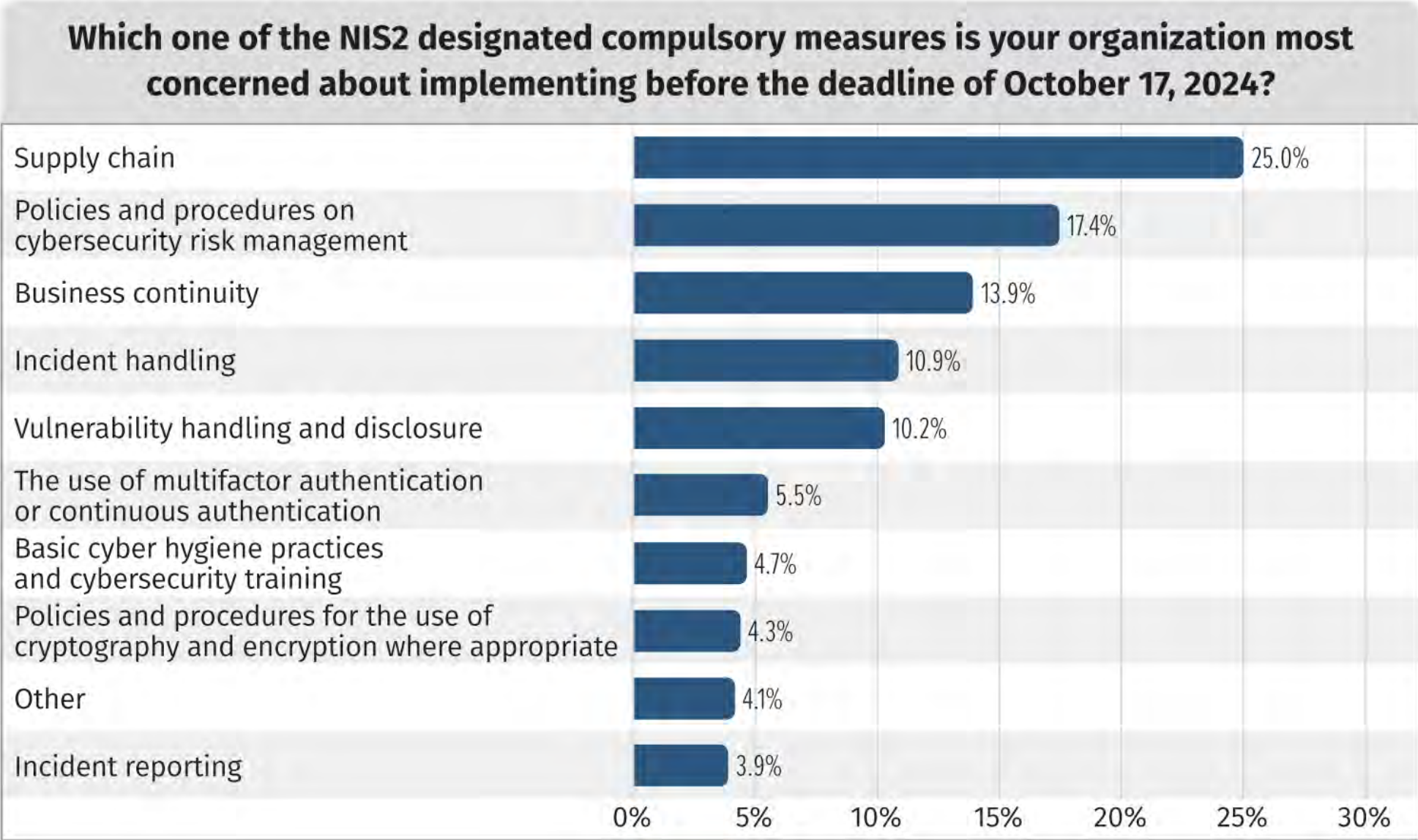
Who in your organization sets policy for security of IT networks?



NIS2 Challenges

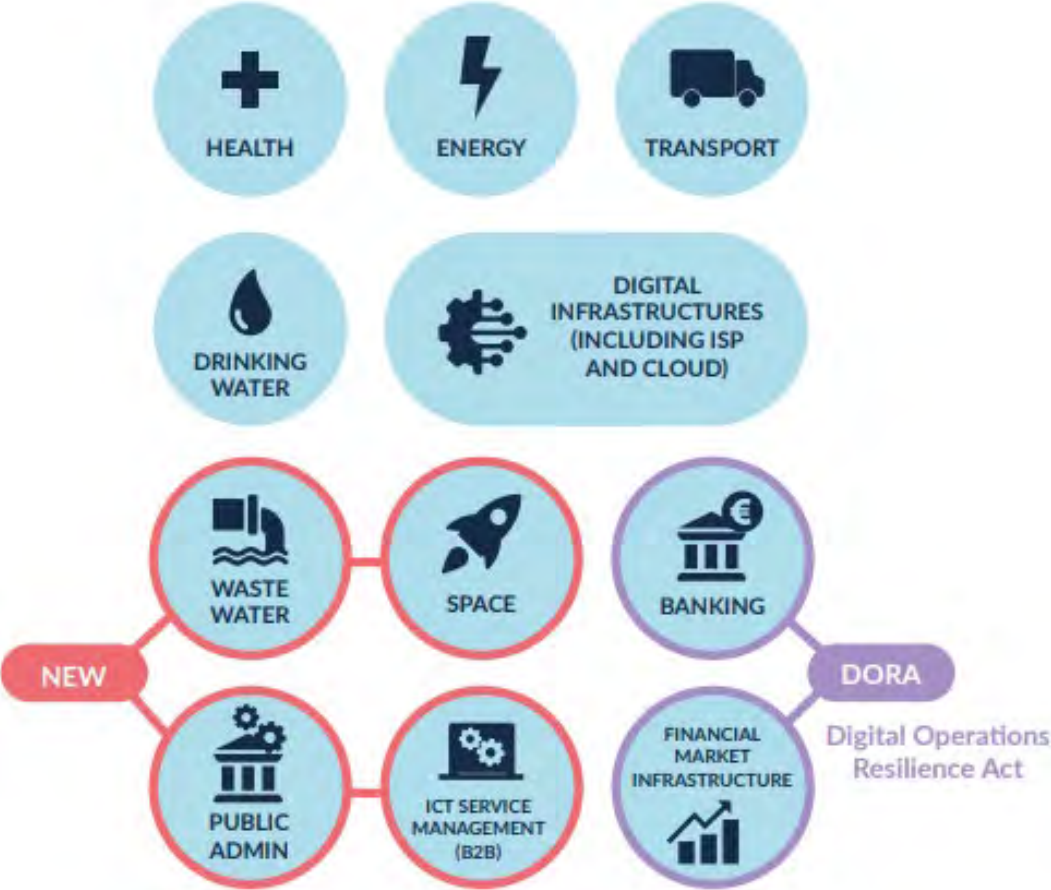


NIS2 Challenges



NIS2 Scoping

Highly Critical Sectors



Critical Sectors



NIS2 Scoping



Scope Assessment

The following questions aim to determine if your organisation may potentially be in scope of the Belgian NIS2 legislation. Depending on its size and the service provided, your organisation may be considered as an **essential** or **important** entity.

[More information about the NIS2 law can be found here](#)

A. Organisation size ("size-cap")

(i) Further information

Please select the size of your organisation before continuing.

These thresholds are calculated on the basis of the figures for the entire legal entity (including all its activities, even outside of the EU), proportionately consolidated with the figures from its partner or linked enterprises.
For more details on the method for calculating these thresholds, see the annex I of Commission Recommendation 2003/361/CE of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, the guide released by the European Commission, or its online tool (linked below).

[Link to Commission Recommendation 2003/361/EC](#)

[Link to the "User guide on the SME definition" from the European Commission](#)

[Link to the SME self-assessment tool from the European Commission](#)

Select your staff headcount range (in full-time equivalents - FTE):	Select
Select your turnover range:	Select
Select your balance sheet total:	Select

Your organisation's size : Please answer all 3 size questions

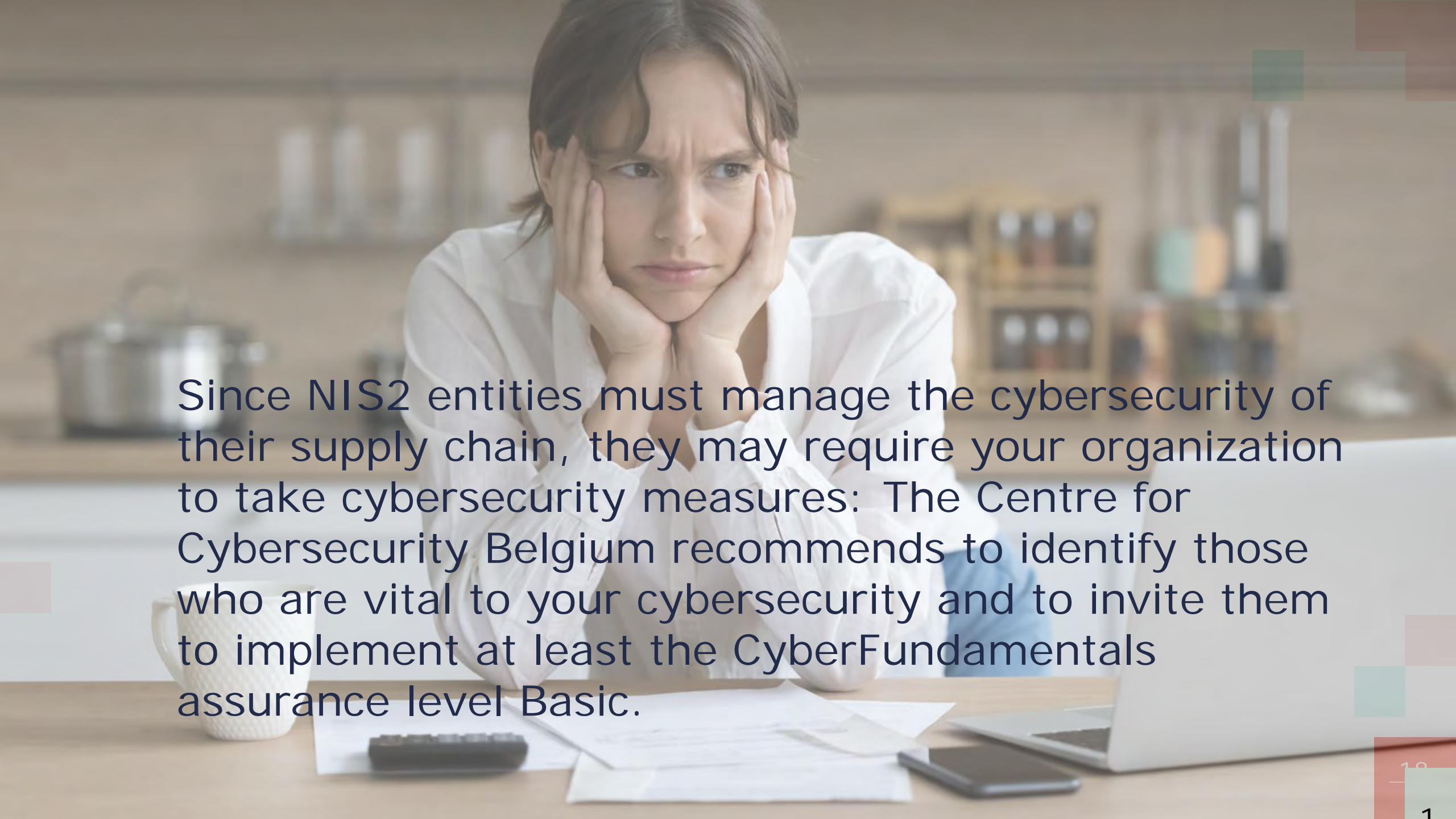
B. Sectors and service provided

Please select at least one sector, or the field 'None of the above' if your organisation does not correspond to any of the sectors, before you can continue.

Banking	
Banking	
Credit institutions	No
Financial Market Infrastructures	
Operators of trading venues	No
Central counterparties (CCPs)	No
Digital	
Digital Infrastructure	
Internet Exchange Point providers	No
DNS service providers, excluding operators of root name servers	No
TLD name registries	No
Cloud computing service providers	No
Data centre service providers	No
Content delivery network providers	No
Qualified trust service providers	No
Non-qualified trust service providers	No
Providers of public electronic communication networks	No





A woman with dark hair, wearing a white shirt, is sitting at a wooden desk. She has a stressed or frustrated expression, with her hands pressed against her cheeks and temples. In front of her is a laptop, some papers, a calculator, and a white mug. The background is a blurred office or home workspace with shelves and various items. The text is overlaid on the image in a dark blue font.

Since NIS2 entities must manage the cybersecurity of their supply chain, they may require your organization to take cybersecurity measures: The Centre for Cybersecurity Belgium recommends to identify those who are vital to your cybersecurity and to invite them to implement at least the CyberFundamentals assurance level Basic.

NIS2 Registration

Access to the portal

Connect with:

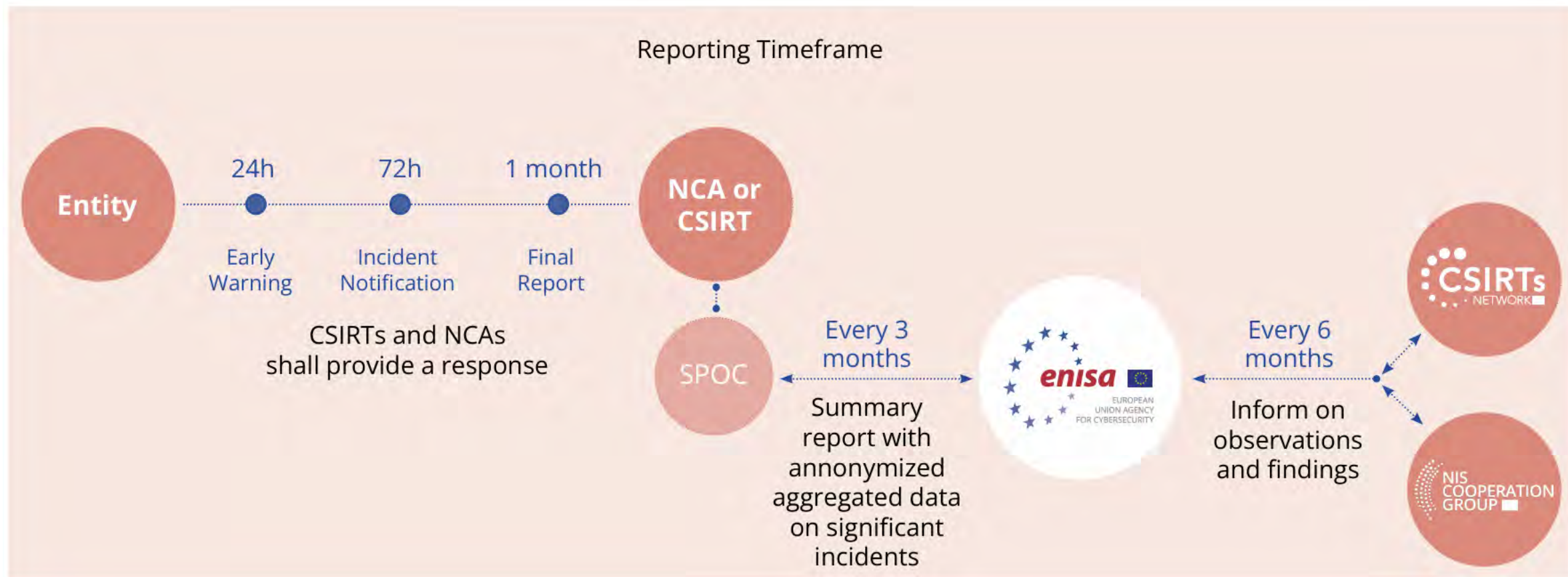


Connect

Eerste registratie

Safeonweb@work is een online overheidsdienst die beschikbaar is voor vertegenwoordigers van bedrijven en organisaties in België en hun afgevaardigden. Om zich te kunnen registreren op Safeonweb@work moet uw bedrijf of organisatie geregistreerd zijn bij de Kruispuntbank van Ondernemingen. Om uw organisatie te registreren bij Safeonweb@work, moet u eerst uzelf of een van uw medewerkers de nodige rol toewijzen op het platform My eGov Role Management voor het beheer van de toegang tot de online platformen van de overheid.

NIS2 Reporting



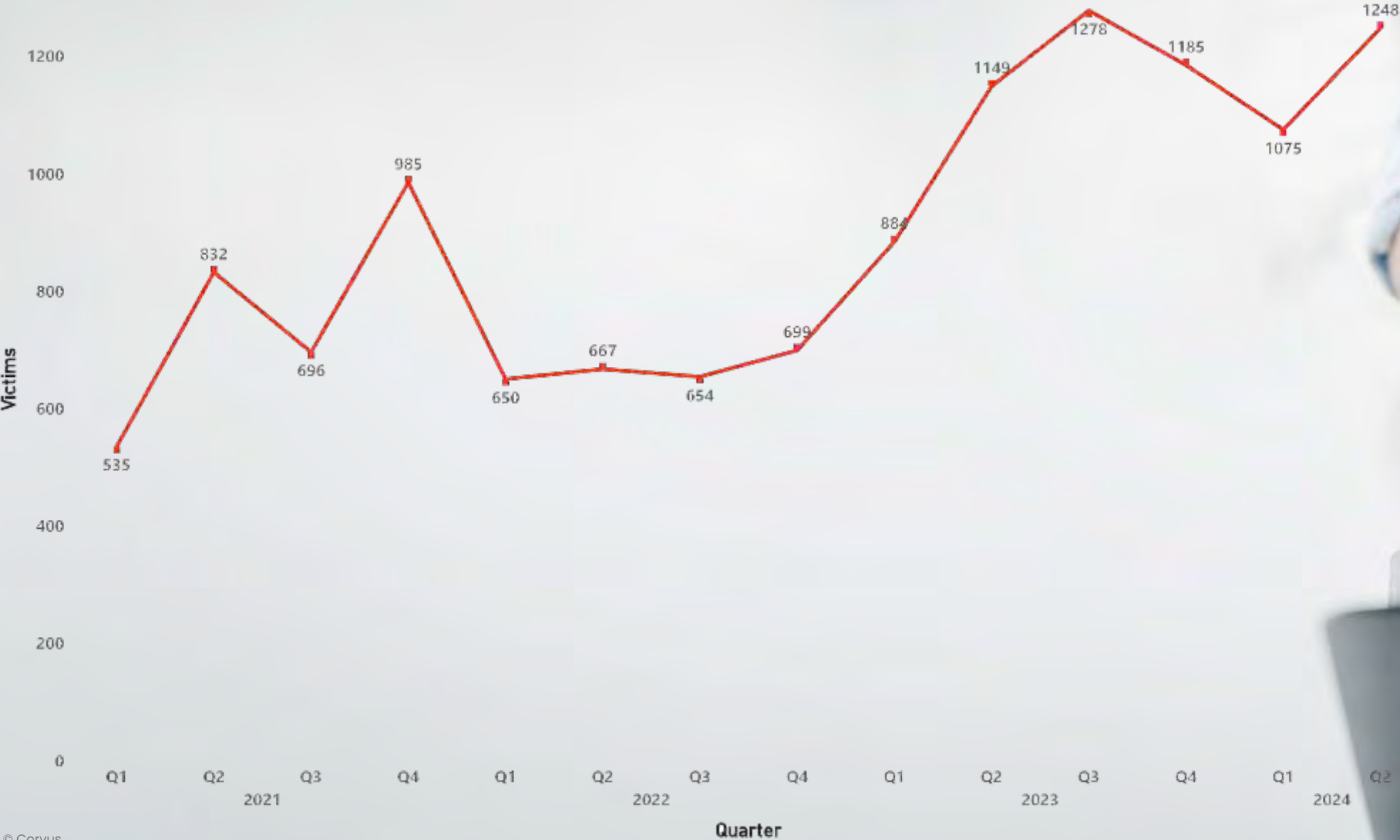
NIS2 Reporting

An incident is **considered significant** and **needs to be reported** in the following **7 situations**

Has caused or is capable of causing:	
	■ 1 Financial loss for the relevant entity that exceeds EUR 500 000 or 5 % of the relevant entity's annual turnover, whichever is lower
	■ 2 The exfiltration of trade secrets
	■ 3 The death of a natural person
	■ 4 A considerable damage to a natural person's health

	■ 5 A successful, suspectedly malicious and unauthorized access to network and information systems occurred, which is capable of causing severe operational disruption.
	■ 6 It is a recurring incident (if it has occurred at least twice within 6 months and the root cause is the same and they collectively meet the financial damage criteria).
	■ 7 The incident meets one or more of the criteria specific for each type of entity in scope the Implementing regulation.

Victims posted to ransomware leak sites



A graphic on the left side of the slide featuring a blue shield with the text 'NIS2' and a keyhole icon. The shield is surrounded by glowing blue lines and a bright blue starburst effect. The background is a gradient of blue and white.

NIS2 Assessment

Challenge:

Without a comprehensive understanding of the current security posture, it is difficult to identify gaps and areas for improvement.

Solution:

We create custom NIS2 compliance roadmaps, designed to meet specific organizational needs, ensuring sustainable and scalable security solutions.

Approach:

We conduct in-depth assessments of current security frameworks, identifying areas of non-compliance and vulnerabilities across IT/OT landscapes.

Why should you do this?

Ensure compliance with NIS2 to avoid penalties. Bolster your organization's ability to detect, prevent, and respond to cyber incidents, protecting critical systems and services.

Let's get started

NIS2 Assessment

We will evaluate your current NIS2 posture, assess the compliance status against the NIS2 guideline and identify any gaps. Based on this, we formulate recommendations for improvements which we then translate into an action plan with clear priorities, timelines and required resources.

Estimated duration: 5 days



Governance

Challenge:

Without proper governance frameworks, identifying, assessing, and mitigating risks becomes a reactive rather than proactive process. Increasing regulations (e.g., GDPR, NIS2) make it difficult to stay compliant without clear processes.

Solution:

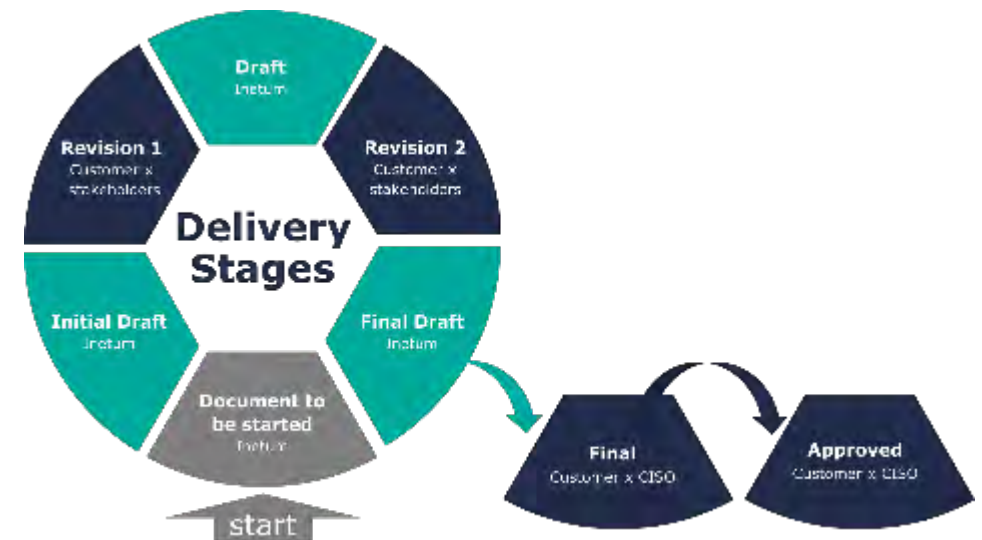
We develop a unified governance structure that integrates regulatory, operational, and risk management processes to ensure clear accountability.

Approach:

Tailoring policies and procedures to align with your specific operational and regulatory requirements, ensuring full coverage of cybersecurity risks. We facilitate collaboration across departments to align policies with business objectives, ensuring security is built into every aspect of operations.

Why should you do this?

A strong governance framework provides visibility into risks, ensuring they are identified, assessed, and mitigated promptly. Well-structured policies align cybersecurity with business strategy, ensuring security doesn't hinder growth but supports it.





Let's secure the
future, together.



Thank you