Samen Digitaal Veilig

SMEs and the supply chain impact of NIS2

Practical implementation lessons

Daan Hoogendijk Director SDV

Samen Digitaal Veilig

MKB Nederland

VNO NCW

IVBB
Instituut voor Verenigingen Branches en Beroepen

Samen Digitaal Veilig

SDV is the largest NIS2 platform in the Netherlands. It was established by and for more than 110 collaborating industry associations to support over 200.000 companies and organizations with cybersecurity.

“Samen Digitaal Veilig is Dutch for Together Digitally Safe”.


IVBB
ONDERZOEKSINSTITUUT
IVBB
IVBB
ONDERZOEKSINSTITUUT
Research
NIS2 impacts security at SMEs
Daan Hoogendijk Director
Impact

RESEARCH

RESEARCH

Who knows this man?

LockBit tactic: gaining access to dozens or even hundreds of other organizations through one weak supplier.

It’s good thing we have Article 21.2(d)

- All hazards
- Systems and physical environment
- Between each entity and its direct suppliers

Article 21

Cybersecurity risk-management measures

1. Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.

Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those 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.

2. The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(a) policies on risk analysis and information system security;

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

Are we fully aware of how large and interconnected the modern supply chain has actually become?

Can NIS2 truly succeed if procurement, SMEs and supply chain ecosystems are not involved?

QUIZ: What percentage of companies have more than 250 employees and what percentage of companies have more than 50 employees?

The Benelux economy is built on small and medium-sized businesses.

Over 97% of companies have fewer than 50 employees.
Less than 1% have more than 250 employees.

The strength of Europe's SMEs comes from craftsmanship and entrepreneurial spirit. Source: Eurostat / EURES

Two practical observations we made

1. Supply chain cybersecurity is significantly larger and more complex than most people realise.

2. The success of NIS2 implementation depends also on large-scale SME adoption.

Why does this matter? Because Europe runs on interconnected supply chains

The combined Benelux market ranks among the world's top 7 import/export economies and approximately 3rd–4th in Europe.

Most affected companies are not formally classified as NIS2 entities but are still vital for the economy and business continuity.

NIS2 Supply Chain security reach is much broader than most people think

In practice, supply chain exposure includes:

IT suppliers

OT suppliers

Physical access suppliers

Maintenance companies

EDI integrations

SaaS dependencies

AI software and internally developed software

ICT & Network Companies

- IT service providers
- Managed Service Providers (MSPs)
- Cloud providers
- Data centers
- Network companies
- Cybersecurity companies
- Software developers
- SaaS providers
- Hosting companies
- Telecommunications companies
- IT audit firms
- And many other ICT suppliers with system access or digital dependencies.

OT-Related Companies

- Machine builders
- Industrial automation companies (OT/ICS)
- Production line suppliers
- Suppliers of digital industrial components
- 3D printing companies
- Smart technology companies
- Factory automation suppliers
- Technical maintenance companies
- And many other suppliers with access to OT environments or operational dependencies.

Companies with Physical Access

- Technicians servicing food-processing machinery
- Technical installation companies
- Electrical and mechanical installation companies
- Warehouse operators
- Container terminals
- Drivers working for transport companies
- Temporary staffing workers
- Third-party facility maintenance providers such as elevator, air-conditioning and solar panel maintenance companies
- And many other physically present suppliers with access to sensitive locations or equipment.

Companies with Digital Integrations (EDI/API)

- Raw material suppliers
- Semi-finished product suppliers
- Chemical companies
- Logistics and transport companies
- Shipping companies
- Aviation suppliers
- And many other companies with API or EDI integrations providing access to sensitive customer systems or operational processes.

Should we include crown jewels related suppliers?

- Accountancy firms
- Consulting firms
- Architectural firms
- Security companies
- Construction companies
- Chemical companies
- Staffing agencies
- Electrical contractors
- Financial advisory firms
- Legal advisory firms
- Logistics companies
- Marketing agencies
- Inventors and IP offices

AI software is growing in every organisation!

- This has major implications
- This was impossible to foresee in 2020
- It will have an effect on every NIS2 entity
- And on every SME
- On every agency
- Everybody

AI is rapidly changing supply chain exposure. SMEs are adopting AI extremely fast

Many AI integrations within operational workflows

AI tools connected to suppliers and customers

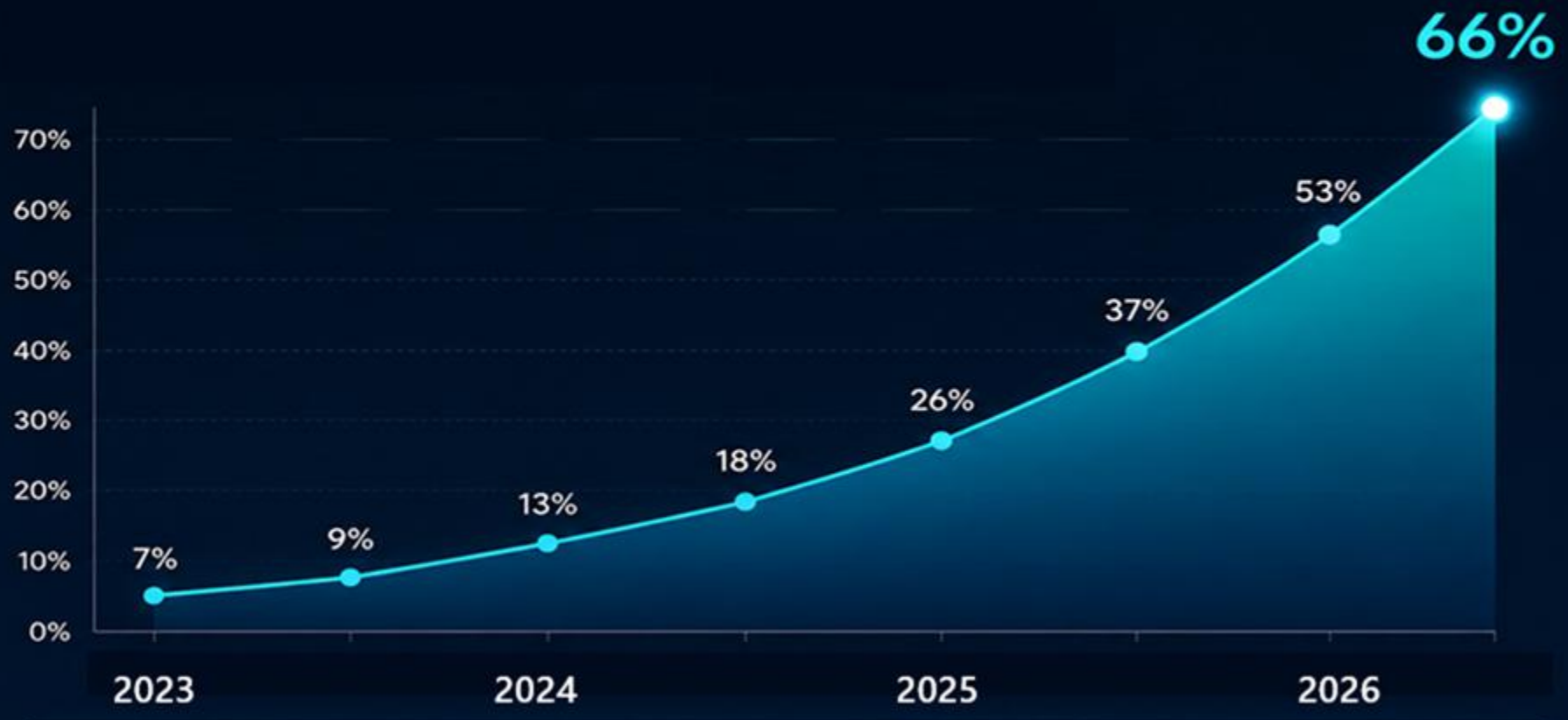
Data flows moving outside traditional visibility

Software dependencies increasing rapidly

Key observation

Many organisations do not yet classify AI usage as a supply chain dependency, while operationally it already is.

THE PRESENCE OF AI IN CORE BUSINESS PROCESSES HAS EXPLODED



AI ADOPTION IN CORE PROCESSES ISN'T JUST GROWING—
IT'S ACCELERATING.

Source: Multiple surveys and industry reports

AI IS NOW PART OF HOW WORK GETS DONE

OPERATIONS
Process automation, predictive maintenance, quality control

CUSTOMER EXPERIENCE
Personalization, chatbots, recommendations, voice AI

FINANCE
Forecasting, fraud detection, intelligent reporting

SUPPLY CHAIN
Demand forecasting, inventory optimization, risk management

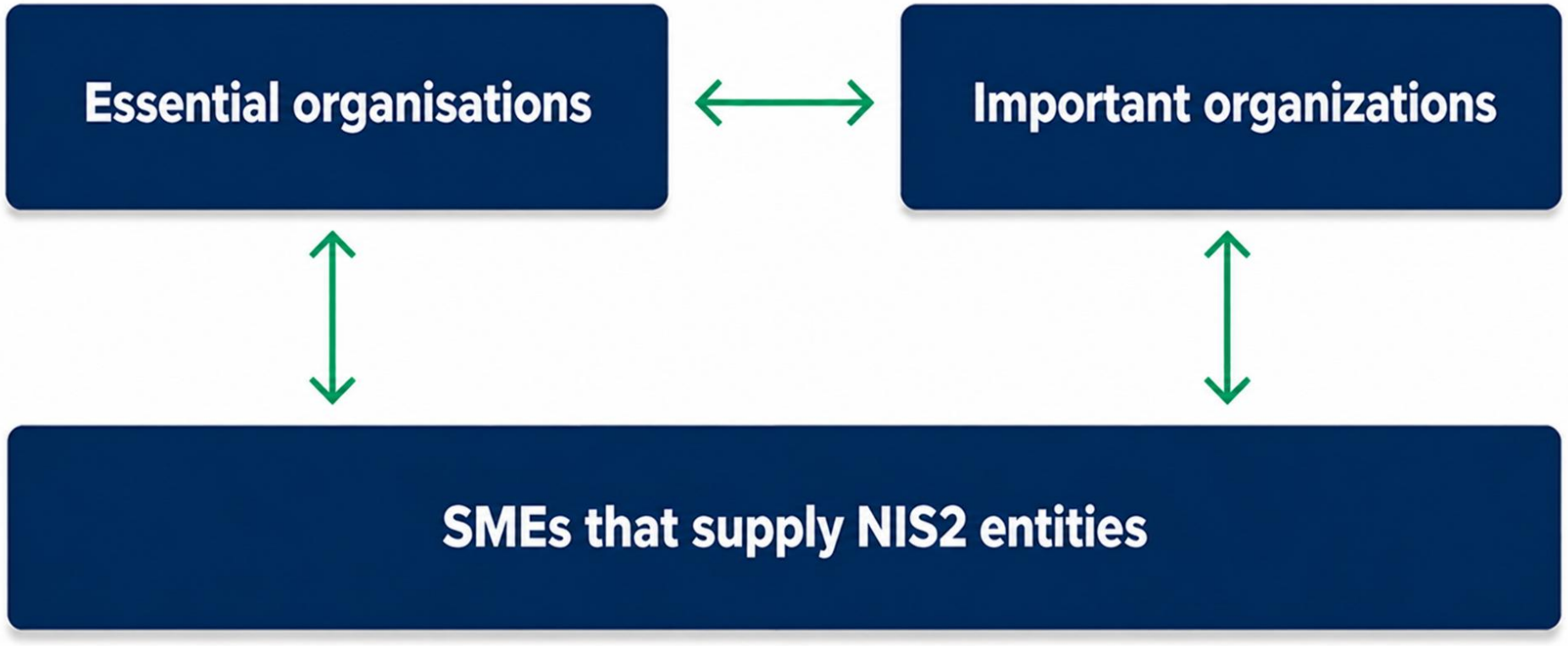
SALES & MARKETING
Lead scoring, content generation, campaign optimization

AI that is used by normal SMEs in primary processes that serve their large customers (NIS2 entities)

ICT / IT	16.000 – 42.000
Installation & Technical Services	1.100 – 4.600
Metal & Manufacturing	600 – 2.200
Transport & Logistics	1.000 – 4.300
Construction	4.000 – 19.000
Facility Services	1.800 – 6.000
Business Services	14.000 – 66.000
HR / Payroll	800 – 3.000
Accounting	3.500 – 9.500
Real Estate / Property Management	500 – 2.200
Security Services	300 – 1.200

NL figures

As a result there are at least 100.000 SME suppliers that may pose cybersecurity risks in the Benelux



How much in the EU?

The SME reality!
Most SMEs think NIS2 will not affect them

What we repeatedly hear:

"We are not a NIS2 entity."

"We are too small."

"We only supply components."

"We are not an IT company."

But in practice:

NIS2 entities increasingly require evidence

Procurement requirements are expanding

Communication at scale for reaching SMEs is an art

Limited cybersecurity awareness, complex terminology

Low engagement with legislation, limited internal expertise

What worked for us:

Sector associations + Activating market ecosystems

Scale

More than 200,000 companies reached through sector ecosystems and market ecosystems.

110 associations activate their 200.000 SME members.

>100 Associations and >100 market partners

ABN·AMRO

EY

kpn

SGS

Kaseya®

kiwa

Allianz

Deloitte.

One of the biggest lessons? Proportionality is essential.

What does not work well:

Overly complex frameworks

One-size-fits-all requirements

Excessive compliance burden

What works better:

Risk-based implementation

Layered maturity models

Supplier-oriented approaches

Key lesson

Without proportionality, SME adoption slows down significantly.

Europe already has many valuable certifications/frameworks

Across Europe we see:

ISO-based approaches

National frameworks

Sector-specific schemes

Different maturity models

Our practical observation

Companies do not want to discard existing investments and certifications.

This is only a small selection of the standards developed by cybersecurity experts and widely adopted across industries.

- ISO/IEC 27001 ISO/IEC 27002
- ISO/IEC 27017
- ISO/IEC 62443
- TISAX
- NEN 7510
- BIO (Dutch Government)
- NIS2 Supply Chain (NIS2 SC 10-20-30)
- CyFun (Cyber Fundamentals)
- Cyber Essentials
- Cyra
- Cyber Trust Austria
- SOC 2
- CIS Controls
- ISA/IEC 62443
- NIST Cybersecurity Framework (CSF)
- NIS2 Supply Chain
- CTPAT
- TAPA TSR / FSR
- European Common Criteria-based Cybersecurity Certification Scheme
- GDPR
- Cyber Essentials
- BSI IT-Grundschutz
- ANSSI frameworks

Mapping reduces friction. Interoperability is more valuable than replacement

What mapping helps achieve:

Less audit duplication, lower implementation costs, faster supplier onboarding, better cross-border scalability, preservation of existing frameworks

Key lesson

Europe benefits from interoperability between certifications/frameworks.

For example, NIS2 SC certification actively promotes and enables this. Preventing duplicate assessments is essential to keep cybersecurity obligations scalable, affordable and practical for large numbers of organizations and suppliers across Europe. ECSO also promotes cross-scheme certification and the avoidance of duplicate certification costs.

NIS2 SUPPLY CHAIN

ECSO 10 YEARS
EUROPEAN CYBER SECURITY ORGANISATION


Samen
Digitaal
Veilig
An SME hack can have major ripple effects.

Our practical implementation approach
Translating principles into operational implementation

Governments communicate:

Basic cybersecurity principles and governance expectations

SMEs ask:

What do we actually need to do? How do we demonstrate it?

Our practical response

Proportional implementation and certification is great for SMEs which are the NIS2 entity suppliers.

EU NIS2 requires large-scale adoption through ecosystems

Effective implementation requires cooperation between:

Governments + regulators + sector associations + auditors + procurement organisations + market parties + the involvement of SMEs

Key lesson

Market ecosystems can significantly accelerate implementation and awareness.

Why we are sharing these lessons
We believe Europe benefits from shared implementation experience

Our position:

We do not see this purely as a national effort, many European countries face similar implementation challenges and practical implementation knowledge should be shared openly.

We are happy to contribute experience regarding and my mail dh@ivbb.nl :

SME communication

Supply chain knowledge

Procurement integration

Proportional implementation

Framework mapping


NIS2
DIRECTIVE
SECURING
SUPPLY CHAINS
TOGETHER
elektro
elektro
GOVERNMENTS
REGULATORS
PRIVATE SECTOR
200,000+
SMES REACHED