The Future of Cyber Resilience in Healthcare – NIS2 Obligations and Sweden's Cybersäkerhetslag

TÜV SÜD

March 2026

Add value.
Inspire trust.

About the Speaker
Richard Skalt

- Currently serves as **Advocacy Manager, Cybersecurity Office at TÜV SÜD**, where he leads external engagement on cyber and AI policy issues, and represents the company in industry associations and standardization bodes global cybersecurity advocacy activities and provides expertise on cybersecurity, tech policy and AI.

- He also serves as **Vice-Chair** of the **AIQI Consortium** and **Advocacy Workstream Lead** at the **Charter of Trust**, helping guide the Alliance's global advocacy on topics ranging from the cybersecurity of products/systems, secure digital infrastructure, and cloud security to AI deployment.

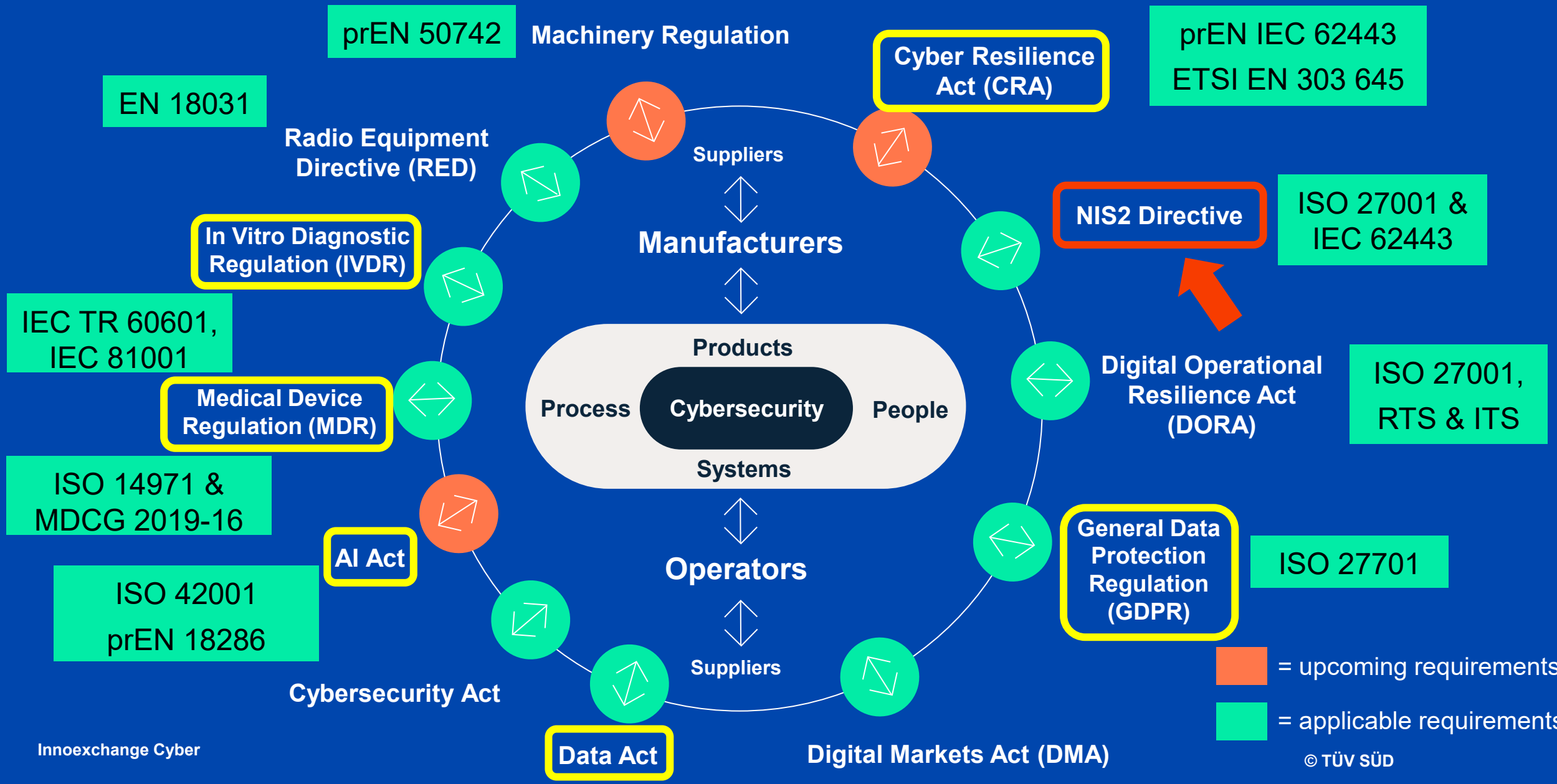
Advocacy Manager, Cybersecurity Office

Charter of Trust

AIQI

The Future of Cyber Resilience in Healthcare –
NIS2 Obligations and Sweden's Cybersäkerhetslag

European cybersecurity regulation framework



The NIS2 Directive at a Glance

What is the NIS2 Directive?

- European Union regulation to enhance overall resilience against cyber threats in the EU and creating a high-level baseline of cybersecurity.
- Updates and expands the original NIS (Network and Information Systems) Directive, strengthening cybersecurity requirements and incident reporting across critical sectors.

What is its current implementation status?

- The NIS2 Directive entered into force in January 2023.
- The deadline for the transposition into national law was 17 October 2024.
- As of October 18, the NIS2 Requirements apply, pending the passing of the national implementation laws (only 5 countries have not done so this far).

Who is affected?

- Organizations across critical sectors in the EU, categorized as “essential” (väsentliga) or “important” (viktiga) entities.

Essential entities:

- Energy
- Transport
- Health
- Financial services
- Water
- Digital infrastructure
- Public administration
- Space

Important entities:

- Manufacturing
- Research
- Waste management
- Food production
- Post and courier
- Chemicals
- Digital providers

Cyber Resilience in Healthcare

Who is affected in the healthcare sector?

Essential entities: Health

- **Healthcare providers** — hospitals, clinics, general practitioners, dental practices, pharmacies, physiotherapy practices, nursing homes providing healthcare
- **Medicinal Research & Development** — pharmaceutical companies, biotech firms, contract research organizations, and academic institutions engaged in the R&D of products

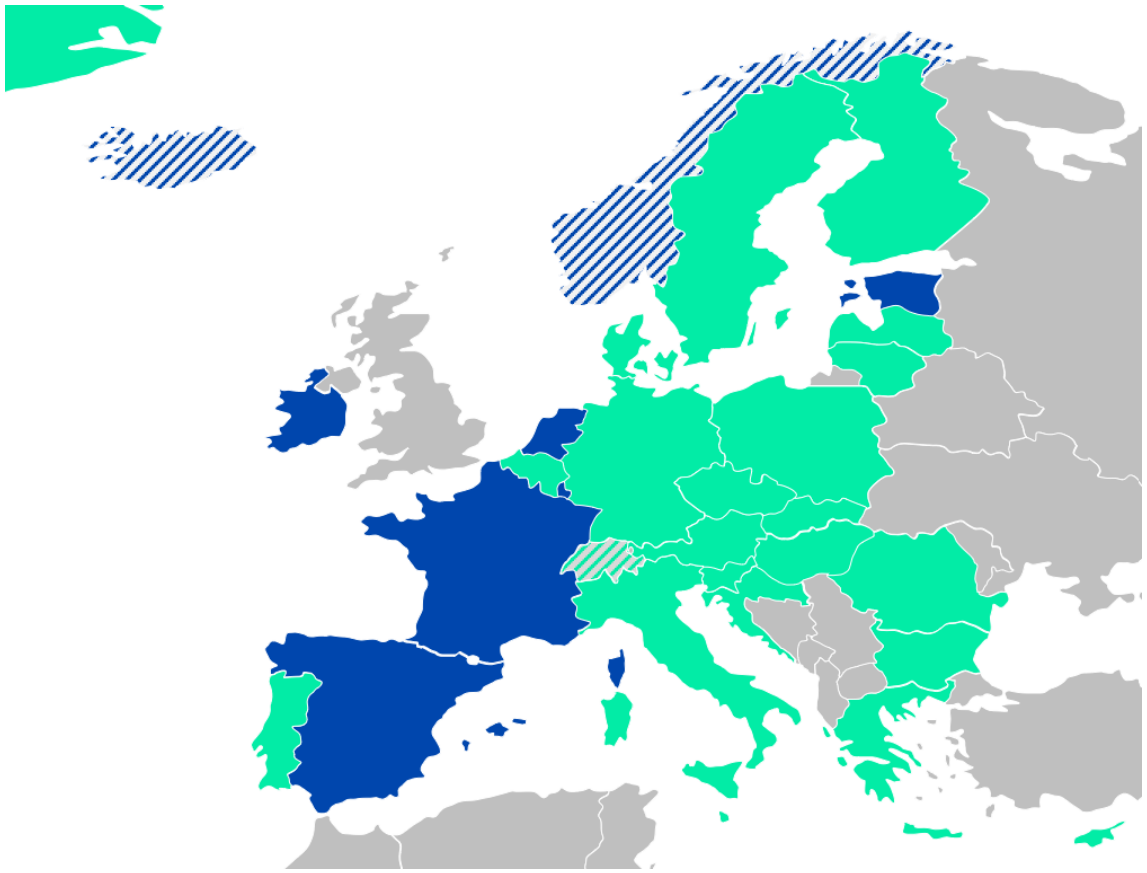
Essential entities: Manufacturing

- **Pharmaceutical Manufacturers** — pharmaceutical manufacturers producing basic pharmaceutical products and pharmaceutical preparations
- **Critical Medical Device Manufacturers** — medical device manufacturers producing devices considered as critical during a public health emergency (according to the public health emergency critical devices list).

Important entities: Manufacturing

- **Medical Device Manufacturers** — Entities manufacturing medical devices (as defined in the Medical Device Regulation (MDR), excluding those already categorized as highly critical.
- **In Vitro Diagnostic Manufacturers** — Entities manufacturing in vitro diagnostic medical devices as defined in the In Vitro Diagnostics Regulation (IVDR)

Status of NIS2 Implementation across the EU



- As of December 2025, most of the 27 EU member states have **fully transposed NIS2 into national law, including Belgium, Croatia, Cyprus, Denmark, Finland, Greece, Hungary, Italy, Latvia, Lithuania, Malta, Romania, Slovakia, Slovenia, …** → on November 28, 2024 the European Commission opened infringement procedures against 23 Member States that had failed to fully transpose NIS2 into national law by this time
- While NIS2 obligations are only enforceable in Member States that have transposed the directive into national law, the obligations are binding in all countries that have the law. **Affected organizations must register and comply in these countries as soon as possible**.
- NIS2 applies extraterritorially, including to companies located outside the EU if they provide services within the EU. Companies - including those based outside the EU - must therefore assess whether NIS2 applies to them.

Implementation Status (as of March 2026)	
	Transposed NIS2 law
	Published proposal

Overview of the NIS2 Implementation Timeline (the case of Sweden)

We are here

14 December 2022	January 2023	18 October 2024	11 December 2025	15 January 2026 - …
▪ A new version of the NIS Directive (NIS2) was issued on December 2022, requiring EU member states to transpose NIS2 into national law within 21 months	▪ The NIS2 Directive official enters into force and confirms the deadline for the transposition of NIS2 into national law to 17 October 2024	▪ The official deadline for the implementation of NIS2 into national law passed, requiring all companies based in EU countries that have passed a NIS2 implementation law to have completed a self-assessment and register at the competent cybersecurity authorities.	▪ The Swedish implementation law was passed towards on 11 December 2025. Upon enforcement, entities falling under scope are expected to have completed their self-assessment and determine whether they fall in scope of the regulation	▪ Companies in scope of NIS2 must register by filling out the official registration form (Anmalningsformula ret) which consists of an excel sheet which must be uploaded to **Myndigheten för civilt försvars e-tjänsteportal** no later than February 16.

NIS2 Requirements for Organizations

Extended Scope

- 7 essential sectors (healthcare, energy, transport, banking, etc.)
- 11 important sectors (postal services, waste management, chemicals, research)
- Threshold: organisations with >50 Employees OR >10 Mio EUR annual turnover

Requirements for Management Bodies

- Approval and oversight of cybersecurity risk mitigation measures (for liability reasons)
- Mandatory cybersecurity training

Stricter Oversight from Authorities

- Mandatory registration with national cybersecurity authorities
- Regular audits (including onsite)
- Financial penalties of up to 10 Mio EUR or 2% of annual turnover

Risk Management Measures

- Risk Analysis and Security Policies
- Cyber Incident Management and Response
- Backup and Crisis Management
- Ensuring Supply Chain Security

Reporting Obligations

- Early Warning: Within 24 hours of discovering a *significant incident* (e.g. high impact, large extent)
- Detailed Report: Within 72 hours
- Final Report: Within one month or upon incident resolution

Other Regulatory Requirements

- Digital Operational Resilience Act (DORA)
- Cyber Resilience Act (CRA)
- General Data Protection Regulation (GDPR)

NIS 2 compliance challenges

Complexity of compliance

Increased scope of obligations

Need for a robust cybersecurity strategy

Continuous monitoring and reporting requirements

Consequences of non-compliance

Hefty fines and penalties

Reputational damage

Operational disruptions

NIS2 Measures applicable to essential & important entities

Governance (Art. 20)

- Management bodies must approve cybersecurity risk measures, oversee their implementation, and are liable for infringements.
- Mandatory cybersecurity training for management and employees to identify risks and evaluate practices.

Cybersecurity Risk Management Measures (Art. 21)

1. Policies on risk analysis & information system security
2. Incident handling (prevention, detection, response)
3. Business continuity & crisis management (incl. backup management & disaster recovery)
4. Supply chain security (suppliers & providers)
5. Security in network & information systems acquisition, development and maintenance
6. Policies & procedures for internal testing, auditing, assessing effectiveness
7. Basic cyber hygiene practices & regular cybersecurity training
8. Policies & procedures for the use of cryptography and encryption
9. HR security, access control policies, and asset management
10. MFA and secure communication systems

Reporting Obligations (Art. 23)

- Entities must notify their CSIRT, the competent cybersecurity authority, and affected service recipients of significant cyber threats as well as inform the latter of recommended responses.
- Incident Notification requirements:
  - Early Warning: Within 24 hours
  - Detailed Report: Within 72 hours
  - Final Report: Within one month or upon incident resolution

Use of European cybersecurity certification schemes (Art. 24)

- The use particular ICT products, ICT services and ICT processes, developed by the essential or important entity or procured from third parties, that are certified under European cybersecurity certification schemes may be required.
- The use of qualified trust services is encouraged.

Benefits of NIS 2 compliance

Enhanced cybersecurity

Strengthens defences, reducing the risk of cyberattacks & data breaches.

Legal compliance

Avoids fines & penalties by adhering to EU regulations.

Operational resilience

Improves business continuity through better incident management & risk mitigation.

Supply chain security

Ensures secure collaboration with third-party vendors.

Reputation protection

Builds trust with customers & stakeholders by demonstrating strong cybersecurity practices.

Improved collaboration

Fosters information sharing & cooperation within sectors & across EU states.

ISO 27001 at a Glance

What is ISO 27001?

- ISO 27001 is a globally recognized standard for information security management.
- Compliance with ISO 27001 demonstrates that your organization has implemented a robust information security management system (ISMS) which protects the confidentiality, integrity, and availability of your information assets and collects all of the relevant information security aspects in one centralized place.

Why consider ISO 27001 for NIS2 / DORA compliance?

- ISO 27001 offers detailed approaches, methodologies, and steps which help to fulfill NIS2 & DORA's broad requirements and is relevant for all companies operating in the EU that handle sensitive information.
- The ISO/IEC 27000 series is directly referenced in section 79 of the NIS2 Directive and covers many requirements already, with the exception of NIS2 and DORA-specific requirements that need to be taken into consideration (e.g. for incident reporting, supply chain security).

Do I need to comply with ISO 27001?

- It is voluntary, meaning organizations choose to comply based on their specific needs, such as meeting customer requirements or improving their security posture in general.

What are typical barriers to ISO 27001 compliance?

- Obtaining ISO 27001 certification is a complex and time-consuming process that makes sense for most essential and important organisations, but is not always practical for their suppliers, as it is too time-consuming and expensive for many SMEs.

ISO 27001:2022 Framework

Scope and Coverage

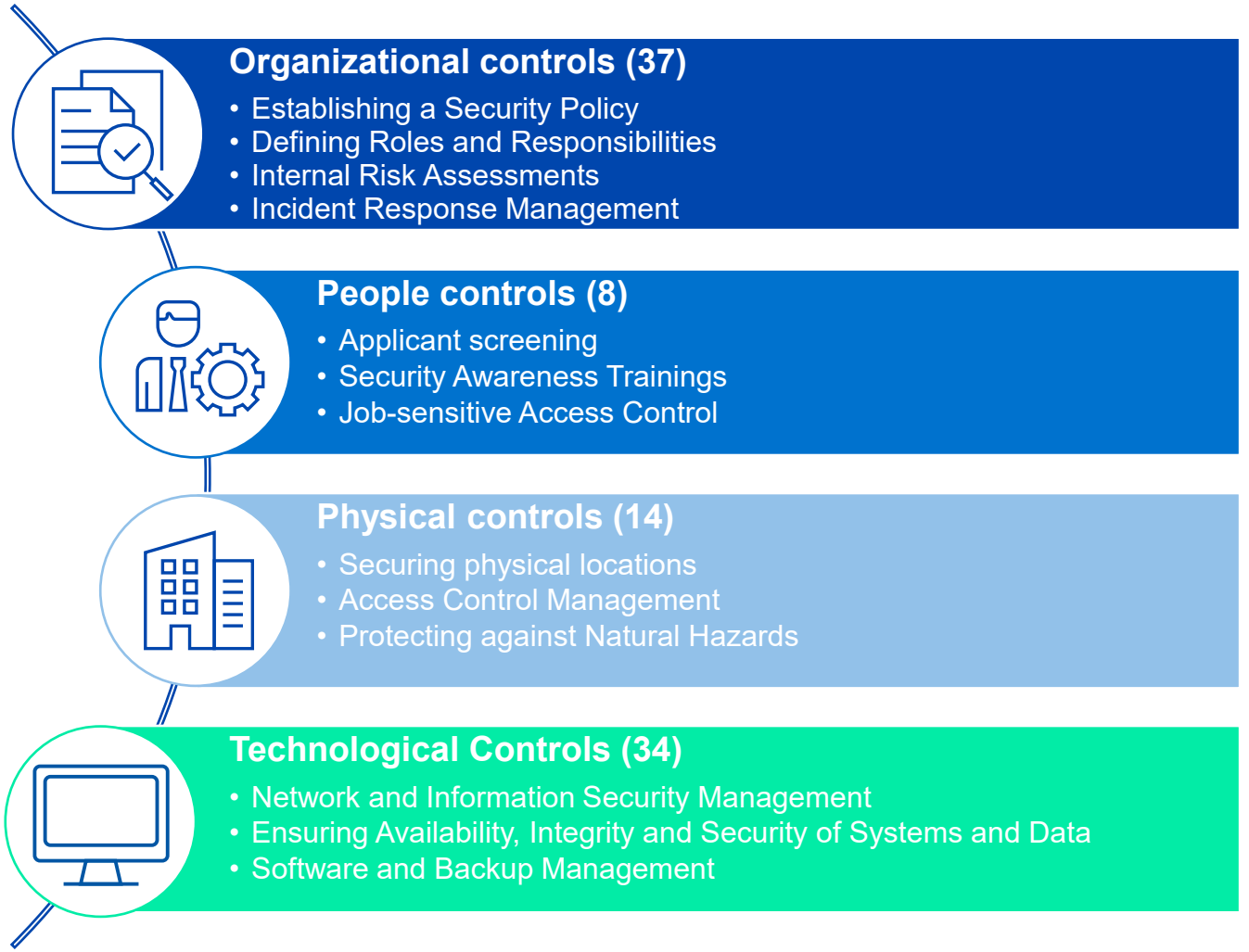
- International framework for establishing, implementing, maintaining, and continually improving an information security management system applicable to any organization, regardless of size, type, or industry.

Framework Structure

- Structured approach with clauses outlining requirements for establishing, implementing, and improving an ISMS

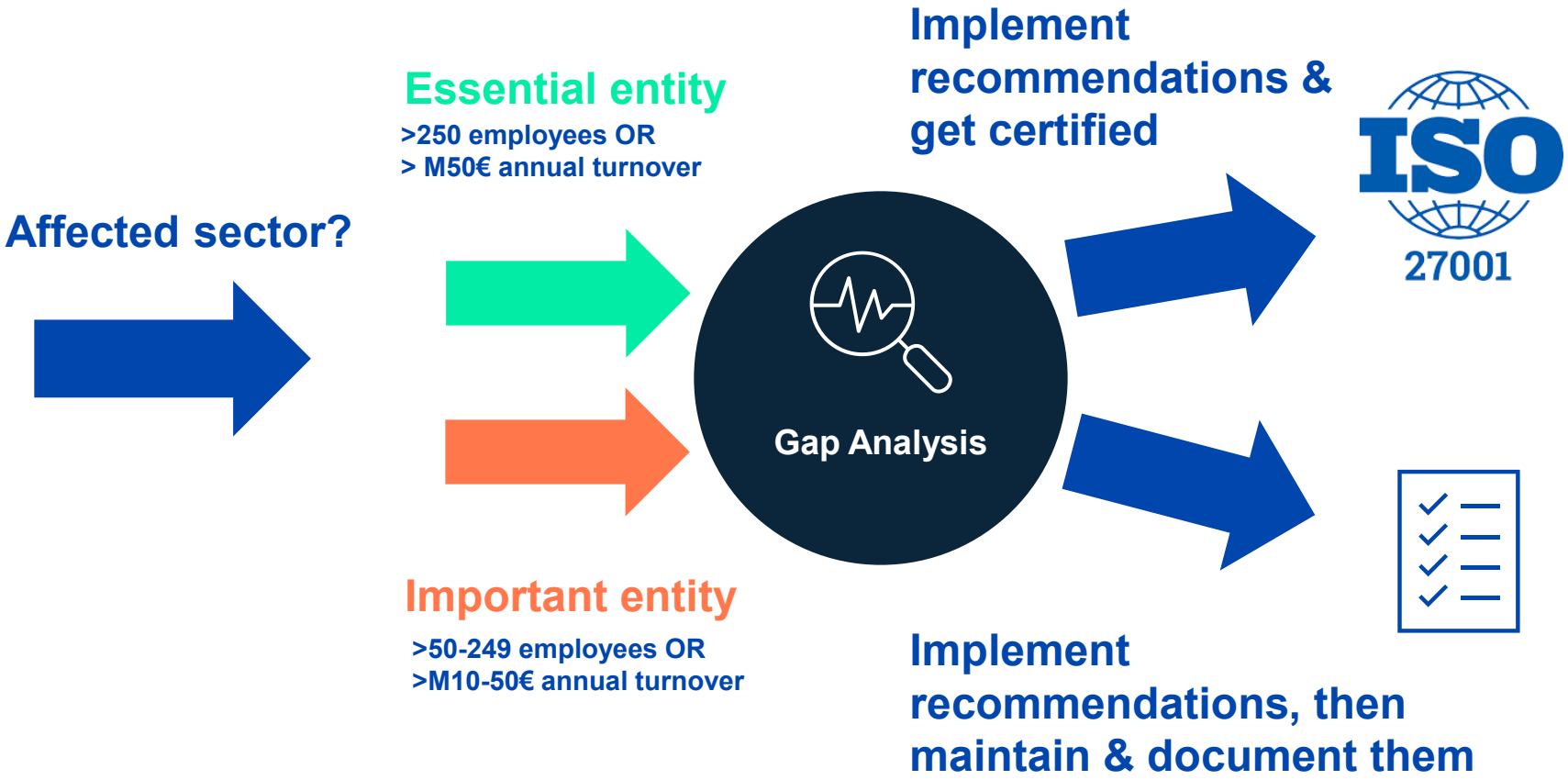
Compliance requirements

- Specifies requirements for organizations to achieve certification, focusing on risk management, security controls, and continuous improvement across 4 domains.



How to demonstrate compliance with NIS 2?

Essential entities are mandated to proactively submit conformity assessments to the national cybersecurity authorities whereas important entities may be asked to submit them when there is evidence or suspicion of non-compliance.



ISO 27001 Certification + NIS 2 conformity

ISO 27001 Certification by an accredited conformity assessment body + maintaining all NIS2 specific requirements

NIS2 conformity

Demonstrable conformity based on closing the gaps identified in the NIS2 Risk Assessment report, and maintaining and continually improving the ISMS

Practical Advice for NIS2 Compliance

Key Requirements for achieving NIS2 Compliance

- Prepare an **extended Statement of Applicability (SoA)**, which expands on the shorter SoA used for ISO 27001 by including NIS2 specific requirements and controls.
- As outlined in ISO 27001, **maintain documentation and governance** by keeping records of compliance efforts, establishing clear roles and responsibilities, training management about NIS2 requirements and conducting regular reviews to stay compliant.
- Register in **Myndigheten för civilt försvars e-tjänsteportal** by indicating which industries your organization belongs to and listing all relevant legal entities falling in scope of NIS2 across all EU member states (and register locally too)
- Remember: **NIS2 does not exist in isolation**
  - Make sure to check which other EU, national, and industry security requirements and standards need to be accounted for in conjunction with NIS2 and ensure that all other relevant requirements and standards (e.g. GDPR, CER, MDR, DORA, IEC 62443) are identified and added to a list of requirements.
- Particular care should be devoted to the **sections most prominently featured in both ISO 27001 and NIS2**, such as:
  - ISMS scope and register of assets
  - Risk identification and assessment, incl. third-party risk management
  - Incident management and notification
  - Vulnerability management
  - Access Control
  - Endpoint and Network Security
  - Information security awareness and cyber hygiene

IEC 62443 at a Glance

What is IEC 62443?

- IEC 62443 is a globally recognized series of standards for industrial automation and control system (IACS) security.
- Compliance with IEC 62443 demonstrates that an organization has implemented robust cybersecurity practices tailored to industrial environments and ensures the protection of industrial systems, components, and data, addressing security throughout the entire lifecycle of automation and control systems.

Why consider IEC 62443 for NIS2 / DORA compliance?

- IEC 62443 provides comprehensive frameworks, methodologies, and best practices that help organizations fulfill the cybersecurity requirements of NIS2, particularly for IACS. It is highly relevant for companies operating in the EU that manage critical infrastructure, operational technology (OT), and industrial networks.
- The IEC 62443 standards align with key aspects of NIS2, addressing risk management, security measures, and supply chain security for manufacturers.

Do I need to comply with IEC 62443?

- Compliance with IEC 62443 is voluntary, but highly recommended for organizations operating industrial automation and control systems and may be required as an industry standard.

What are typical barriers to IEC 62443 compliance?

- Obtaining IEC 62443 certification can be complex and time-consuming, particularly for organizations with extensive industrial automation and control systems. Smaller suppliers and SMEs might struggle to implement the security controls due to the significant investment required in terms of time, cost, and expertise.

IEC 62443 Framework

Scope and Coverage

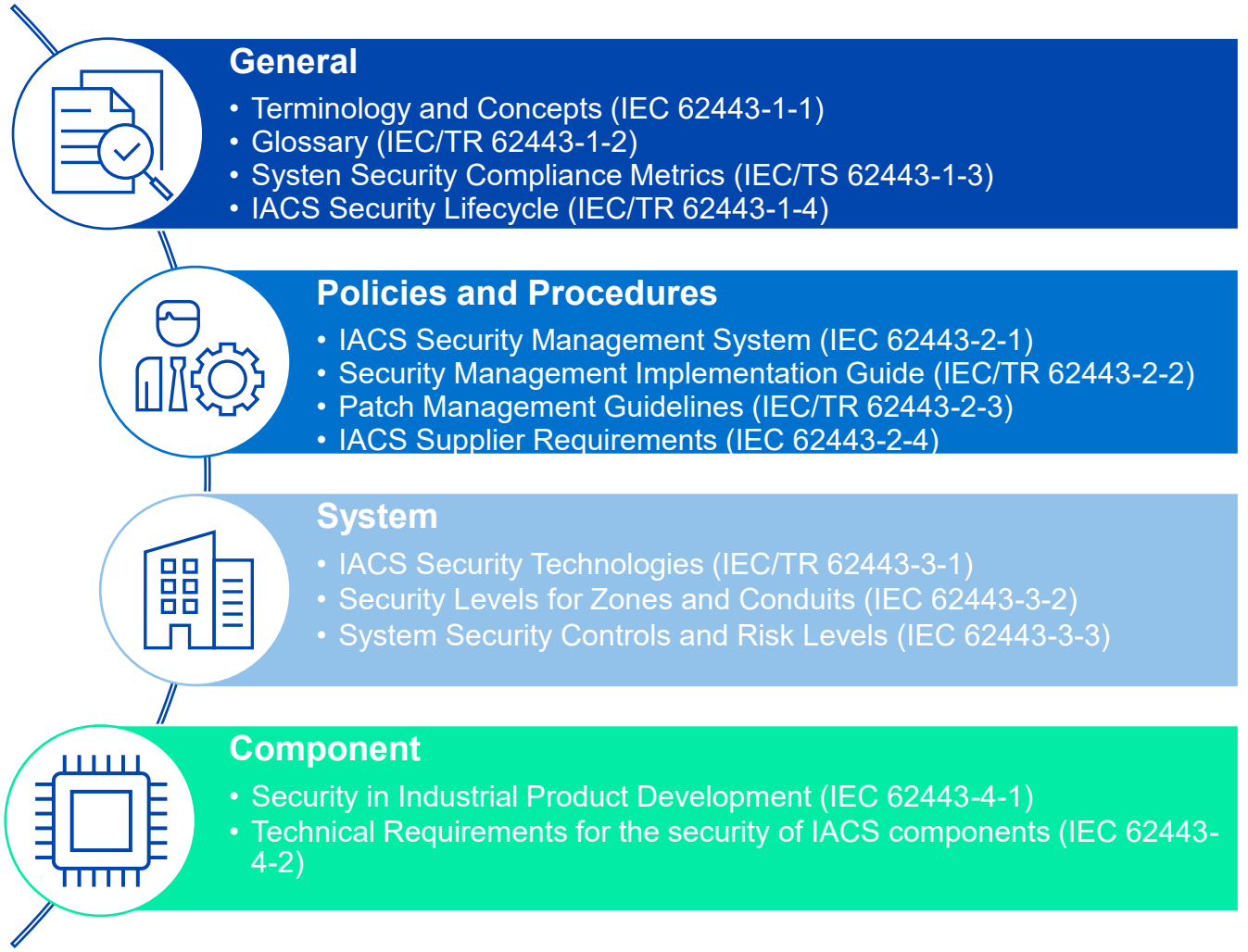
- Cybersecurity standard for industrial automation and control systems (IACS), addressing risks for asset owners, system integrators, and product suppliers across industries like manufacturing, energy, and healthcare. Covers hardware, software, networks, and organizational security measures.

Framework Structure

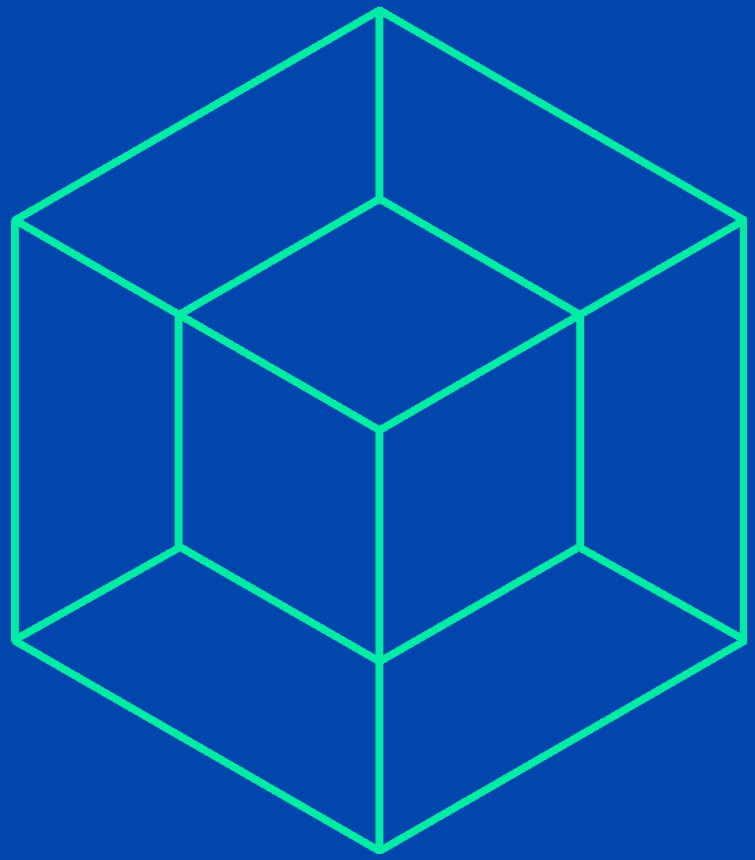
- Uses a risk-based, defense-in-depth approach to protect industrial systems, divided into four categories:
  - general concepts (IEC 62443-1-…),
  - policies and procedures (IEC 62443-2-…),
  - system-level security (IEC 62443-3-…),
  - And component-level security (IEC 62443-4-X).

Compliance requirements

- Organizations must assess risks, implement security controls, define security zones, follow secure development practices, monitor threats, and undergo security assessments to meet IEC 62443 requirements.



Thank you!



Contact us at
info@tuvsud.com

TÜV SÜD

Follow us on:

tuvsud.com
info@tuvsud.com