Cybersecurity & Compliance
NIS2 is in force

NORDUnet Conference 2026

2025-09-09

Björn Sjöholm - bear@unidot.se

Abstract

- ✓The NIS2 Directive is now in force, introducing stricter cybersecurity and governance requirements for organizations across critical and important sectors within the EU.
- ✓This presentation provides an overview of how compliance and cybersecurity responsibilities within organizations need to be aligned. The challenges from overlapping requirements across multiple regulations will be addressed.
- ✓We will discuss common compliance challenges and provide practical tips on how to manage them effectively.

Björn Sjöholm

Cyber Security Entrepreneur

bear@unidot.se

Cyber Security, IT-Security, Information Security
Advisor, Auditor, Trainer, Business leader

M.Sc. Comp.Sci.
CISA, CISM, CRISC, CISSP
ISO 27001 Lead Auditor

unidot

Linkedin: linkedin.com/in/bjornsjoholm

Agenda

- NIS2 Overview
  - Key Requirements
  - NIS2 Timeline and Implementation status
- Challenges
  - Regulatory overlaps
  - Governance and Responsibilities
  - Risk-based vs Rule-based
  - Incident reporting and Third-party risks
- How
  - What is important?
  - What are the risks?
  - Compliance and Trust

NIS2 Directive

Who – What - Timeline

NIS2 – Who: Critical sectors

Essential Entities

- Energy
- Transport
- Banking
- Financial market infrastructures
- Healthcare
- Drinking water
- Wastewater
- Digital infrastructure
- ICT service management (e.g., managed service providers)
- **Public administration**
- Space sector

Important Entities

- Postal and courier services
- Waste management
- Manufacturing
- Chemical production and distribution
- Food production, processing and distribution
- Digital providers
- **Research organizations and certain educational institutions**

NIS2 – Who - continued

Size

- Employ 50 or more people, or
- Have an annual turnover or balance sheet total exceeding €10 million

And …

- Providers of public electronic communications networks
- Trust service providers
- DNS service providers
- TLD registry operators
- Certain critical digital infrastructure providers

NIS2 – Article 21
Cybersecurity risk-management measures

1. "… manage the risks …"
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… , and crisis management
   d) supply chain security
   e) … systems acquisition, development and maintenance, including vulnerability handling …
   f) … assess the effectiveness of cybersecurity risk-management measures
   g) basic cyber hygiene practices and cybersecurity training
   h) .. use of cryptography and encryption;
   i) human resources security, access control policies and asset management;
   j) … use of multi-factor authentication or continuous authentication solutions … secured emergency communication systems

NIS2 What – Article 21

Appropriate and proportionate technical, operational, and organizational measures

- Governance & Risk
  - Policies on risk analysis and information system security
  - Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
- Resilience & Operations
  - Incident handling
  - Business continuity, backup management, disaster recovery, and crisis management
- Technology & Protection
  - Security in acquisition, development, and maintenance of network and information systems
  - Policies and procedures regarding the use of cryptography and encryption
  - Multi-factor authentication (MFA) or continuous authentication, secured communications, and secure emergency communications systems
- People & Third Parties
  - Supply chain security
  - Basic cyber hygiene practices and cybersecurity training
  - Human resources security, access control policies, and asset management

Timeline

The Directive required Member States to apply the national implementing measures from 18 October 2024

Country	Implementation status
Finland	Cybersecurity Act entered into force 8 April 2025.
Denmark	NIS2 Act entered into force 1 July 2025.
Sweden	Cybersecurity Act entered into force 15 January 2026.
Estonia	NIS2 implemented through amendments to the Cybersecurity Act, entering into force during 2025/2026 implementation phases.
Norway	NIS2 is not yet fully implemented and is being incorporated through national legislation and EEA processes.

No NIS2 implementation in place
France
Spain
Ireland
Norway – not yet implemented NIS2 in Norwegian national law

Challenges

Challenges – Multiple regulations

Challenges - Governance

- ✓You need a governance framework
  - “We have an ISO 27001 ISMS – are we NIS2 compliant?”

- ✓The management body own the risk
  - ✓Shall approve and oversee cybersecurity risk-management and measures
  - ✓Identify what’s critical
  - ✓Set risk tolerance
  - ✓Monitor risks over time

Challenges - Riskbased vs. Rulebased

Riskbased

- Risk determines mitigation and control measure

Risk treatment:

- Risk mitigation
- Risk transfer
- Risk acceptance
- Risk avoidance

Rulebased

- Mitigation and controls are defined externally or internally
- Defined by
  - Requirements / Criteria
  - Rules
  - Defined specific controls

Challenges – Incident reporting & Third party risks

- Incident reporting
  - 24-hour early warning and subsequent reporting
- Supply-chain risk & Third party management

Challenges – Example Sweden

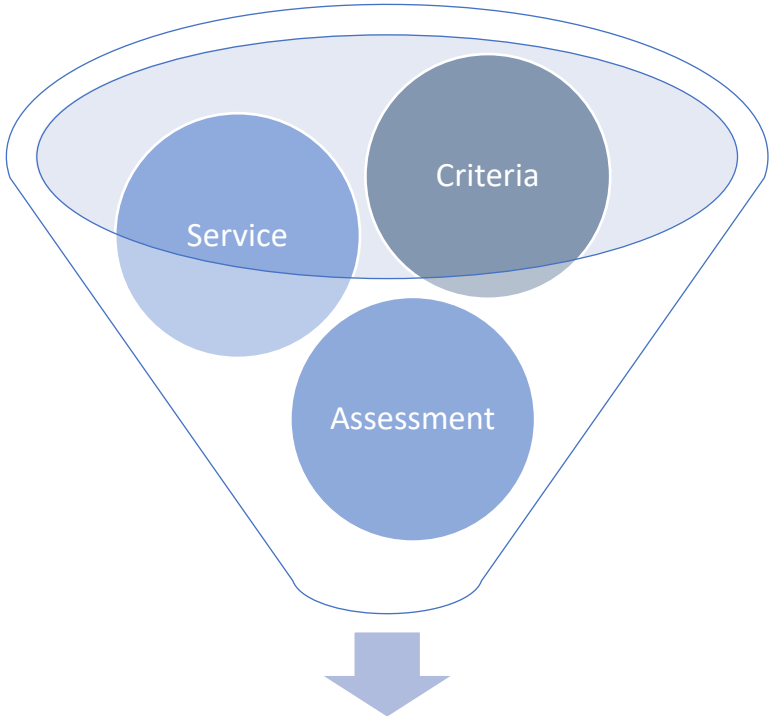
- Multiple Supervisory Authorities (Competent Authorities)
  - An organisation could have several different Supervisory Authorities if it a critical or essential entity in several sectors?
- The Swedish Cybersecurity Act applicability
  - The law applies to the whole organisation and not just the critical services
  - The law applies to all municipalities
- Detailed regulations (föreskrifter)

Sweden – Regulation (föreskrifter) – status

- MCFFS 2026:1 - Notification – applies since 2 February 2026
- MCFFS 2026:8 - Incident reporting – applies since 1 July 2026
- **MCFFC 2026:11 -Security measures and security training for leadership**
  - will apply 1 October 2026
- MCFFS 2026:12 Security audit and vulnerability scanning
  - will apply 1 October 2026

How

Compliance & Trust

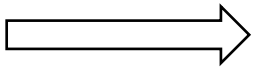


Compliance is handling another party's risk

Adhering to requirements or set of controls in a standard, contract or regulation

What is important?

- What are our services and assets?
  - Information
  - Products
  - Services
  - Physical equipment

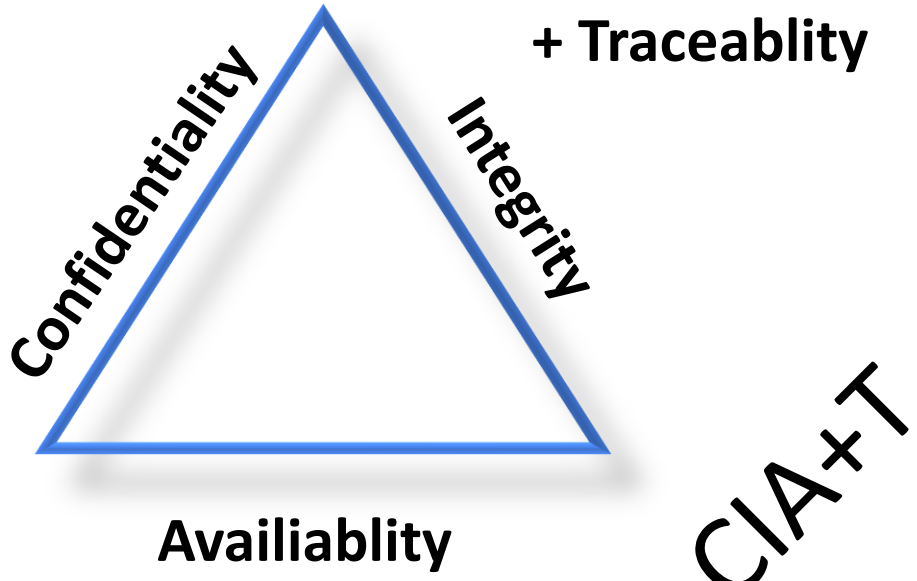


- ✓ NIS2 + National implementation
  - ex. Cybersäkerhetslagen (Sweden)
- ✓ CER
- ✓ CRA

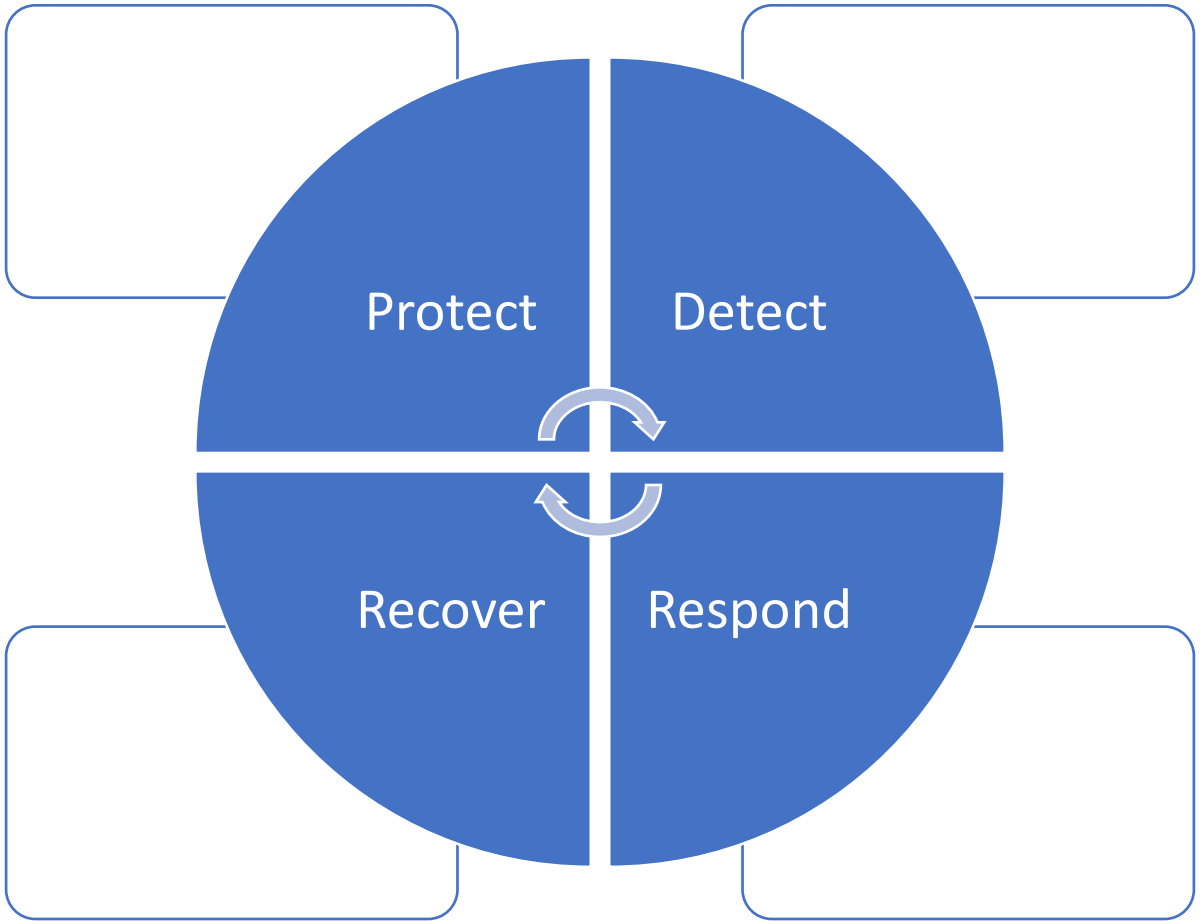
- Executive Management decides what is critical and important

What are the risks?

- What assets do we have?
- What aspects are important?

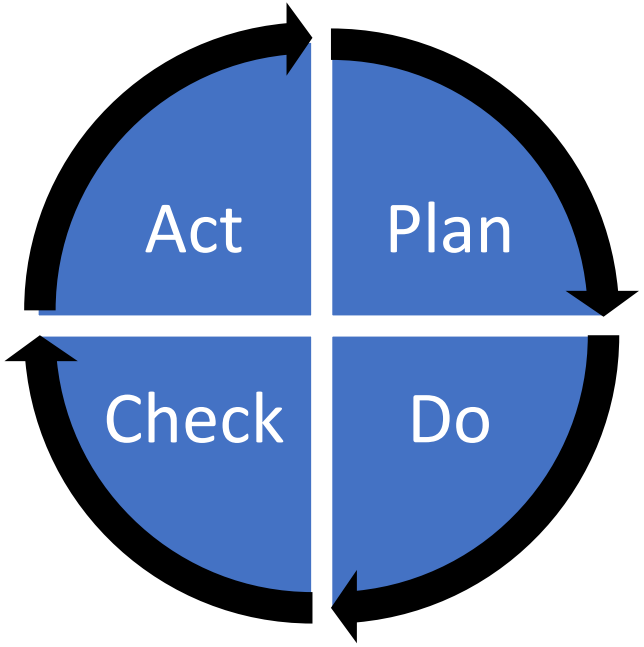


Cybersecurity measures



Information Security Management System

- The work should be carried out in a structured manner
  - With management support
    - Identify what needs protection
    - Defined risk acceptance
- Ensure that the organization
  - operates efficiently,
  - complies with legal requirements, and
  - is continuously improved.



Questions & Answers

Cybersecurity & Compliance
NIS2 is in force

NORDUnet Conference 2026

2025-09-09

Björn Sjöholm - bear@unidot.se