Sweden's implementation of the NIS2 Directive

In response to the European Union's Network and Information Security Directive (NIS2), Sweden has implemented this landmark cybersecurity framework into national law through the new **Cybersecurity Act (Cybersäkerhetslagen, 2025:1506)** and the **Cybersecurity Ordinance (Cybersäkerhetsförordningen, 2025:1507)**, which entered into force on **15 January 2026**.

The NIS2 Directive, adopted at EU level in late 2022, was designed to modernize and significantly expand cybersecurity requirements across critical infrastructure and essential societal services, including digital infrastructure, energy, transport, health, finance and other key sectors.

In Sweden, the directive has been transposed through the new Cybersecurity Act, which integrates the core NIS2 principles:

- Risk management and cybersecurity measures
- Incident reporting obligations
- Leadership accountability
- Broader scope covering more sectors and entities

The Act replaces Sweden's older NIS1-based framework and elevates national cybersecurity requirements to align with the EU's updated expectations.

The entry into force on 15 January 2026 marks the point at which Swedish organisations must align with the new NIS2-based requirements. In parallel, Swedish authorities — including the **Myndigheten för civilt försvar (MCF)**, which plays a coordinating role in the national implementation — have been preparing for supervision, registration processes and compliance support.

What NIS2 Means for Swedish Organisations

Under the new law, entities classified as **essential** or **important** — depending on sector, size and societal impact — will be obligated to:

- Implement documented risk management and cybersecurity measures
- Report significant incidents within prescribed timeframes
- Engage senior management directly in cybersecurity governance
- Assess and manage supply-chain risks

These rules introduce stronger regulatory oversight and more substantial consequences for non-compliance compared to Sweden's previous NIS framework.

While the legal framework is now in force, additional details and sector-specific guidance from supervisory authorities will continue to develop in parallel with registration and oversight processes. The law applies across a broad range of sectors defined by NIS2, including **digital infrastructure** — a category that is closely linked to many systems and services used by fire safety and security providers.

Fire safety & security industry

Although NIS2 and the Cybersecurity Act are often discussed through an IT and cybersecurity lens, the practical consequences for the fire safety and security industry are increasingly significant. While many fire safety and security companies may not be directly classified as essential or important entities, their technologies and services are increasingly intertwined with the compliance needs of regulated customers — particularly through supply-chain expectations and operational resilience requirements.

Convergence of physical and cyber resilience

Many fire safety and security systems today are networked and software-driven — from advanced fire detection panels to integrated access control and alarm management platforms. These systems:

- Generate, transmit and store information over networks
- Form part of customers' operational processes
- Can influence continuity of essential services

Under NIS2-based cybersecurity legislation, resilience is defined broadly and includes both cybersecurity and operational continuity. This means systems critical to detecting and responding to emergencies are increasingly considered part of the wider resilience and cybersecurity landscape.

Incident reporting and operational continuity

Fire detection, suppression systems, intrusion alarms and other security technologies often serve as early warning systems for incidents that could affect operations, safety or service availability. If a cyber or operational incident impacts such systems at a covered entity (for example, in digital infrastructure, critical manufacturing, or essential service providers), the incident may need to be:

- Detected quickly
- Classified accurately
- Reported to authorities within mandated timeframes

Compliance therefore requires that physical safety and security systems are reliable, integrated with incident reporting workflows where relevant, and capable of supporting broader organisational resilience.

Supply chain and third-party expectations

Even when fire safety and security providers are not directly regulated entities under NIS2, they will increasingly be part of the compliance chain for organisations that are. Customers with cybersecurity obligations will expect:

- Robust cybersecurity capabilities in supplied systems
- Secure remote maintenance and service procedures
- Clear documentation and lifecycle support
- Alignment with recognised standards and best practices

This trend reflects NIS2's strong focus on supply-chain security — a key theme for organisations with dependencies on network-connected infrastructure and external service providers.

Practical impacts on Swedish stakeholders

For manufacturers

- Design products with cybersecurity in mind (secure defaults, patch management, and logging).
- Support customers with incident-ready documentation and integration support.

For integrators

- Embed risk assessments and incident logging into system design and delivery.
- Understand how customer compliance obligations may shape technical and contractual requirements.

For service providers

- Ensure service level agreements (SLAs) reflect reporting timelines and risk management expectations.
- Provide training and guidance on how fire and security system data can support resilience and incident response.

For end-users

- Prioritise fire and security systems in corporate risk management and business continuity planning.
- Involve fire/security functions in incident response routines and cybersecurity governance.

Holistic resilience

Sweden's implementation of the NIS2 Directive represents a decisive shift toward holistic resilience — one that blends cybersecurity, operational continuity, and physical protection. Organisations that understand and adapt to this convergence will not only meet compliance requirements but also strengthen the safety and reliability of the environments they protect.

For members of the fire safety and security sector, this development underscores the critical role their technologies and expertise play — not merely in safety compliance, but in supporting the broader resilience and security of Sweden's digital and physical infrastructure.

www.euralarm.org