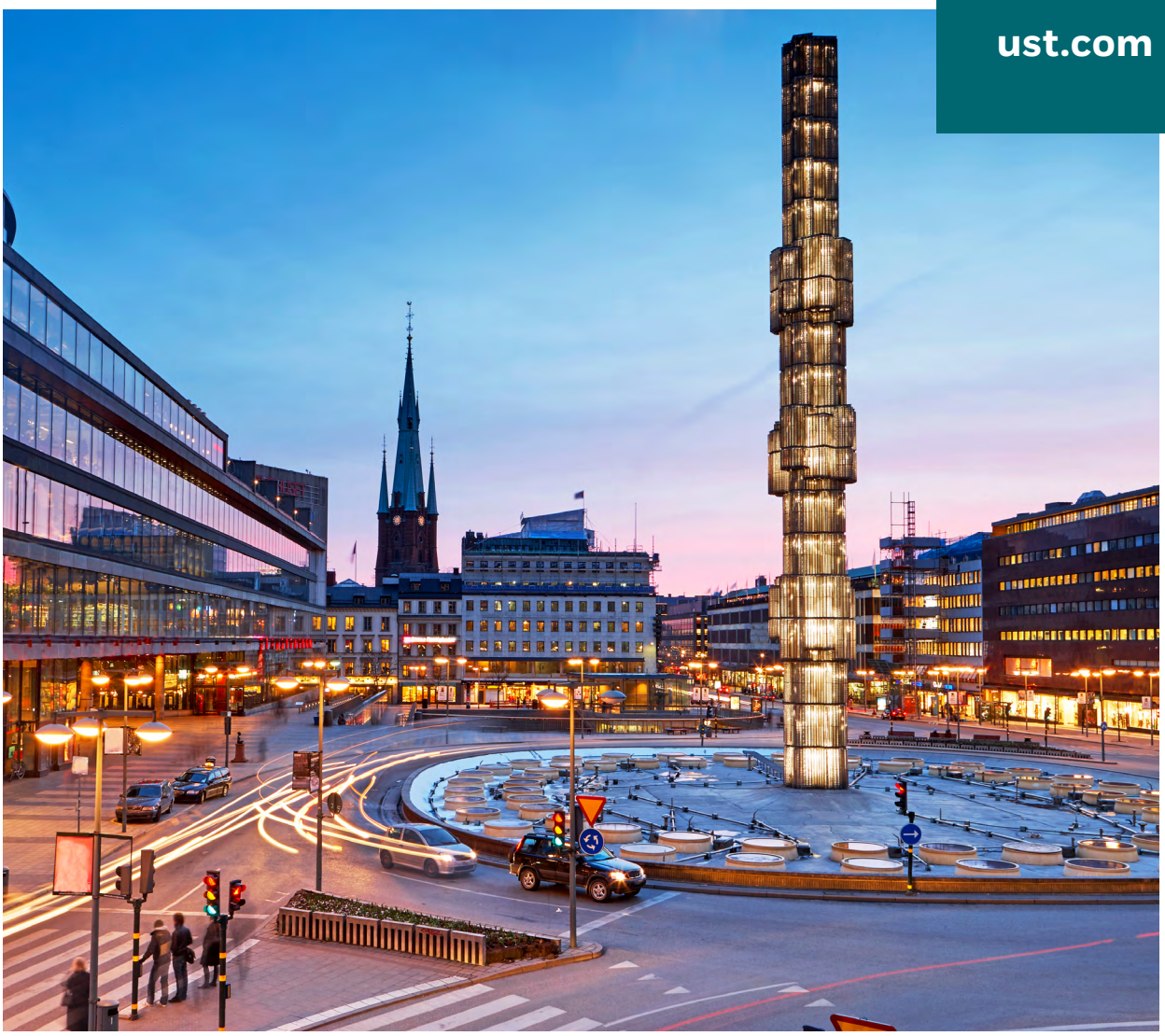
NIS2 is here

WHITEPAPER

What Sweden's Cybersecurity Act means for your business

ust.com



UST

Table of contents

Executive summary

What Sweden's Cybersecurity Act means for your business, and how to turn a new legal baseline into genuine resilience.

15 Jan. 2026 Act in force	**18** sectors in scope	**24h / 72h** incident reporting clock	**€10M** max fine, essential entities

Sweden has moved cybersecurity from an IT concern to a board-level legal obligation. The headline points for decision-makers:

- **The law is live**. The Cybersecurity Act (Cybersäkerhetslag, SFS 2025:1506) took effect on 15 January 2026, transposing the EU NIS2 Directive and repealing the 2018 NIS Act. [1]
- **Scope widened sharply**. Coverage expanded from 7 to 18 sectors, and a "whole-entity" rule means the entire organisation is in scope once any qualifying part is. [2]
- **Thresholds are clear**. Entities in listed sectors with 50+ employees or €10M+ turnover or balance sheet are covered; certain providers are covered regardless of size. [2]
- **The clock is tight**. Significant incidents require a 24-hour early warning, 72-hour notification and one-month final report; registration with the supervisory authority is mandatory. [3]
- **The stakes are personal**. Fines reach €10M or 2% of global turnover for essential entities and €7M or 1.4% for important entities, with personal management liability and possible management bans. [4]

The grace period is over. For more than a year, Swedish boards treated NIS2 as a deadline somewhere on the horizon. That horizon has arrived. On 15 January 2026, the Cybersecurity Act (Cybersäkerhetslag, SFS 2025:1506) entered into force, transposing the EU NIS2 Directive into Swedish law and repealing the 2018 NIS Act. The substantive duties, security measures and incident reporting, have applied from day one, not from some later phase-in date.

This whitepaper is written for the people now accountable for that shift: CISOs, CIOs, general counsel, and the board members who, for the first time, can be held personally responsible for cybersecurity governance. It explains what changed, who is covered, what the law demands, what non-compliance costs, and the practical sequence of work that turns a legal obligation into operational resilience.

Why this matters now

Sweden is one of Europe's most exposed cyber targets, and the data is not subtle. Cyberattacks against Swedish organisations rose roughly 70% in the first quarter of 2025 compared with the same period in 2024, a sharper increase than any Nordic neighbour, making Sweden one of the most-attacked countries in the EU. [5]

The threat is no longer abstract. In August 2025, a ransomware attack on a single HR-software supplier, Miljödata, cascaded across the public sector, disrupting services at 164 municipalities and four regions, with around 250 client organisations affected in total. [6] The ransom demanded was small, about 1.5 Bitcoin. The disruption was nationwide. It was a textbook demonstration of supply-chain risk, and exactly the failure mode NIS2 is designed to address.

THE SIGNAL FOR LEADERSHIP

Sweden's national defence planning now names cyberattacks as a central threat to national security. The Swedish cybersecurity market is forecast to grow from about USD 1.53 billion in 2025 to USD 2.44 billion by 2030. [7] The regulatory pressure and the threat curve are rising together, and the law now expects you to be ahead of both.

What actually changed on 15 January 2026

If you operated under the old NIS Act, four shifts matter most. None is cosmetic.

1. FROM SEVEN SECTORS TO EIGHTEEN

The previous law covered seven sectors. The Cybersecurity Act covers eighteen, spanning Annex I and Annex II of NIS2: energy, transport, banking, financial market infrastructure, health, drinking and waste water, digital infrastructure, ICT service management, public administration, space, postal and courier services, waste management, manufacturing of critical products, food, chemicals, research, and digital providers. In practice, almost the entire Swedish public sector, including municipalities and regions, is now covered.

2. THE WHOLE-ENTITY PRINCIPLE

This is Sweden's most distinctive choice. Under the old regime, only the specific service that triggered regulation had to comply. Now, once any qualifying part of an organisation falls in scope, the entire legal entity is covered. You cannot ring-fence compliance to one business line; the obligation reaches across your whole IT footprint, including HR, finance, and administrative systems.

3. ACCOUNTABILITY MOVED TO THE BOARDROOM

The Act places cybersecurity squarely at executive and board level. Senior management must approve and oversee risk-management measures and undergo cybersecurity training. For serious infringements committed intentionally or through gross negligence, a court can bar a named individual, a board member or CEO, from holding management functions for between one and three years. Cybersecurity is now a personal-liability matter, not a back-office cost line.

4. MANDATORY REGISTRATION AND A STRICT REPORTING CLOCK

In-scope entities must self-identify and register with the relevant supervisory authority. Sweden's registration portal opened on 2 February 2026, and supervisory action is possible where registration is not made promptly. The substantive duty to report significant incidents has applied since the Act came into force, regardless of registration status.

Are you in scope?

Two tests decide baseline coverage: a sector test and a size test. If you meet both, you are almost certainly in scope. Some providers are covered regardless of size.

Test	What it means for you	What it means for you
Sector	Any of the 18 designated sectors	Operating in a listed Annex I or II sector is the first trigger.
Size	50+ employees, or €10M+ turnover or balance sheet	Aligns with the EU SME definition; medium and large entities are the focus.
Special criteria	Regardless of size	Trust service providers, DNS/ TLD providers and parts of digital infrastructure are always covered.
Public sector	Municipalities and regions covered	Sweden extends coverage beyond EU minimums to public administration.

Essential or important? In-scope entities are classified as either essential (large operators in critical Annex I sectors, qualifying electronic-communications and trust providers, public authorities) or important (most others). The core obligations are similar, but supervision is more proactive, and maximum fines higher, for essential entities.

The ten minimum security measures

The Act requires “appropriate and proportionate” technical, operational and organisational measures, sized to your actual risk, not a fixed checklist. They cluster into ten areas every in-scope entity must address:

- Risk analysis and information-system security policies
- Incident handling, detection and response
- Business continuity, backup management and crisis management
- Supply-chain security, including supplier and service-provider relationships
- Security in acquisition, development and maintenance of systems
- Procedures to assess the effectiveness of security measures
- Basic cyber hygiene practices and security training
- Policies on cryptography and, where relevant, encryption
- Personnel security, access control and asset management
- Use of multi-factor authentication and secured communications

A useful shortcut: if you hold ISO 27001:2022 certification, you already cover a large share of these controls. The common gaps are incident-reporting workflows, board-level governance and training documentation, and extending scope beyond the existing ISMS boundary to the whole entity.

The incident reporting clock

When a significant incident occurs, the timeline is fixed and tight. Build your processes around it before you need them, not during a live event. [3]

Deadline	Obligation
Within 24 hours	Early warning to the supervisory authority that a significant incident has occurred.
Within 72 hours	Fuller incident notification with an initial assessment. (24 hours for certain trust service providers.)
On request	Intermediate status updates as the authority requires.
Within 1 month	Final report: root cause, severity, impact, and mitigation taken.

A practical detail with financial consequences: timely notification is often a condition of cyber-insurance cover. Align your CERT-SE reporting procedures with your insurer's notification requirements so a reporting delay does not also void a claim.

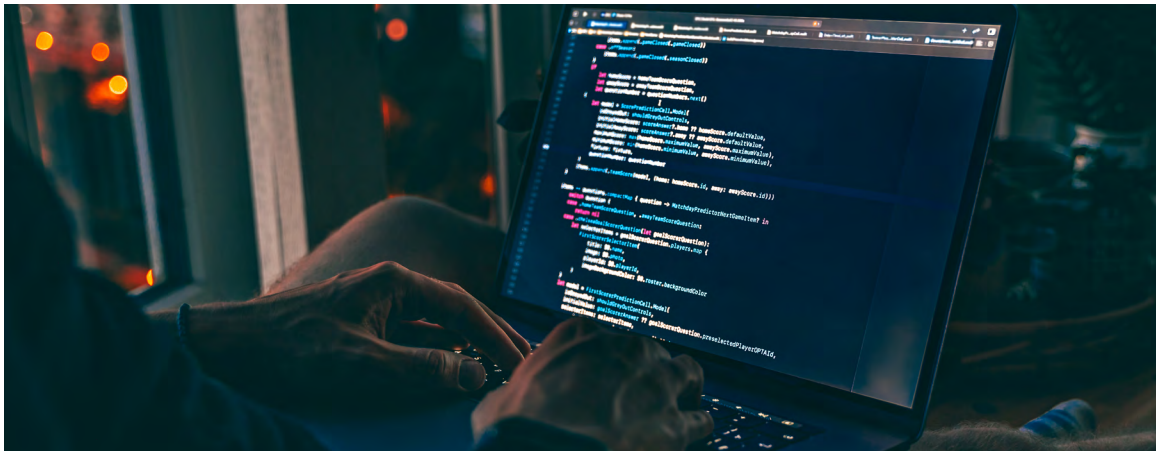
What non-compliance costs

Sweden adopted the maximum penalty levels the directive permits,one of the most stringent enforcement frameworks in the EU. The fines are only part of the exposure. [8]

Classification	Maximum administrative fine
Essential entities	Higher of €10,000,000 or 2% of total global annual turnover
Important entities	Higher of €7,000,000 or 1.4% of total global annual turnover
Public operators	Up to SEK 10,000,000
Minimum fine	SEK 5,000

Beyond the fine. Authorities can issue formal reprimands, binding orders, and "name-and-shame" publication requirements. For serious, intentional or grossly negligent failures, a court can disqualify named executives from management roles for one to three years. Where personal data is involved, a single incident can draw penalties under both the Cybersecurity Act and the GDPR.

A practical 90-day path to compliance



Compliance maturity typically takes between four and twelve months depending on your starting point. The first 90 days are about establishing position, closing the highest-risk gaps, and demonstrating due diligence. UST sequences the work in four moves.

01

Confirm applicability and register

Run a qualified scope analysis against the sector and size tests, classify the entity as essential or important, and complete registration with the supervisory authority. Account for overlap with the Protective Security Act and, for financial entities, DORA.

02

Gap assessment against the ten measures

Map current controls to the ten areas. If ISO 27001 is in place, prioritise the known gaps: incident-reporting workflow, governance and board training, and whole-entity scope extension.

03

Stand up the reporting and governance machinery

Implement the 24h/72h/one-month reporting workflow with named roles, board-level cyber-risk reporting, and leadership tabletop simulations so decision-making is rehearsed, not improvised.

04

Operationalise continuous resilience

Move from project to operating model: 24/7 threat detection and response, supply-chain security assessment, and recurring effectiveness reviews that produce the documented evidence regulators expect.

How UST helps Swedish organisations

UST brings global engineering depth and local accountability to NIS2, from first assessment through to fully managed security operations. Our CyberProof practice partners with security and leadership teams to build resilience that goes beyond compliance: **risk-posture assessment, board-level reporting, 24/7 managed detection and response, incident response and crisis management, supply-chain security, and leadership tabletop simulations.**

The principle behind every engagement is simple: demonstrate value before asking for commitment. We begin with a structured diagnostic and a focused proof-of-value sprint, so you understand precisely what you are investing in before scaling, with Sweden-based programme leadership maintaining continuity throughout.

MAP YOUR NIS2 GAPS BEFORE THE REGULATOR DOES.

Start with a CyberProof NIS2 Readiness Assessment, a structured evaluation of your scope, obligations, and highest-risk gaps, delivered as a prioritised action plan rather than a sales presentation.

Speak with a cybersecurity specialist

Sources and further reading

This whitepaper draws on Swedish government sources and legal analysis current as of mid-2026. Numbered references correspond to the markers throughout the document. Figures are summarised for context; verify specifics against primary sources before acting.

1. Swedish Energy Agency — New Cybersecurity Act enters into force (15 Jan 2026); Act 2025:1506 and Ordinance 2025:1507. https://www.energimyndigheten.se/en/news/2026/new-cybersecurity-act-enters-into-force-in-sweden/

2. CMS Law-Now — NIS2 implemented into Swedish law by the new Cybersecurity Act (scope, 18 sectors, size thresholds, fines). https://cms-lawnow.com/en/ealerts/2025/12/nis2-to-be-implemented-into-swedish-law-by-the-new-cybersecurity-act

3. Deloitte — NIS2 Now in Force: Sweden's Registration Portal Opens; ten minimum security areas; phased regulations. https://www.deloitte.com/se/sv/services/legal/perspectives/nis2-now-in-force.html

4. Advokatfirman Lindahl — New Cybersecurity Act: reporting obligations and administrative fine levels. https://www.lindahl.se/en/expertise/national-security-trade-control/new-cybersecurity-act-implementation-of-the-nis2-directive-in-swedish-law/

5. U.S. ITA / trade.gov — Sweden Cybersecurity: ~70% rise in attacks Q1 2025 (Check Point Research). https://www.trade.gov/country-commercial-guides/sweden-cybersecurity

6. Euro Weekly News — Miljödata ransomware: 164 municipalities and four regions, ~250 client organisations. https://euroweeklynews.com/2025/09/02/sweden-held-to-ransom-164-councils-confirmed-and-more-paralysed-after-cyber-strike/

7. Research and Markets — Sweden Cybersecurity Market: USD 1.53B (2025) to USD 2.44B (2030). https://www.researchandmarkets.com/reports/6074234/sweden-cybersecurity-market-share-analysis

8. ECSO — NIS2 Directive Transposition Tracker (sanction levels, sector-specific authorities). https://ecs-org.eu/activities/nis2-directive-transposition-tracker/

Primary legal instruments: Cybersecurity Act (SFS 2025:1506) and Cybersecurity Ordinance (2025:1507); Government Bill Prop. 2025/26:28; supervisory authority — Swedish Civil Defence and Resilience Agency (MCF / MSB).

This document is for general information only and does not constitute legal advice. Obligations depend on your specific circumstances; consult qualified counsel.

Together, we build for boundless impact

Since 1999, UST has worked side by side with the world's best companies to make a powerful impact through transformation. Powered by technology, driven by AI, inspired by people, and led by our purpose, we partner with our clients from design to operation. Our AI-driven digital solutions, proprietary platforms, engineering, R&D, products, and innovation ecosystem turn core challenges into impactful, disruptive business outcomes. With deep industry knowledge and a future-ready mindset, we infuse expertise, innovation, and agility into our clients' organizations—delivering measurable value and positive lasting change for them, their customers, and communities around the world. Together, with 30,000+ employees in 35+ countries, we build for boundless impact—touching billions of lives in the process.

ust.com

Version 0101-20260722

U ▪
S T