Congenius

Horizontal Directives & Regulations Series

# NIS 2 (Cybersecurity) Directive (EU) 2022/2555

*August 2024*

*By Jörg Dogwiler*

*Edited by Hannah Matthews*

# Overview & Transition Periods

On 27 December 2022, Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the EU (NIS 2 Directive) was published in the Official Journal of the European Union.

After entering into force on 16 January, Member States need to now adopt and publish the measures necessary to comply with the NIS 2 Directive by 17 October 2024, as the Directive will apply from **18 October 2024**.

NIS 2 replaces the current NIS Directive (Directive (EU) 2016/1148), setting out a regulatory framework for cybersecurity. All medium and large organisations (those with more than 50 employees or more than €10 million yearly turnover) operating within the KRITIS sectors covered by the Directive (for which the medical device sector is included), or those which provide services covered in the Directive, fall within its scope. This includes healthcare providers, pharmaceutical companies, and manufacturers of medical devices considered critical in a public health emergency.

# How will medical device manufacturers be impacted?

## Appropriate & proportionate risk management measures

According to Article 21 in the Directive (Cybersecurity risk management measures), qualifying organisations must take appropriate and proportionate technical, operational, and organisational measures to:

- **Manage the security risks posed to their network and information systems used for operations or service provision**

- **Prevent or minimise the impact of incidents on recipients of their services and on other services**

The measures should ensure a level of security that's appropriate to the risks posed, taking into consideration:

✓ The "state-of-the-art"
✓ Relevant European and international standards
✓ The cost of implementation

During their proportionality assessment of the measures to take, organisations should consider their size, their exposure to risks, and the likelihood and potential severity of incidents – including any societal and economic impact.

NIS 2 mandates that management must approve the cybersecurity risk management measures taken by their organisation, and that members of the management must follow specific training before subsequently providing training to their employees.

# How will medical device manufacturers be impacted?

## An “all-hazards approach”

Organisations are advised to ensure that the measures they take are based on an **“all-hazards approach”** that aims to protect their network and information systems and the physical environment of those systems from security incidents. The measures should cover the following as a minimum:

| | |
|---|---|
| **Secure your network & IS acquisition, develop & maintain where necessary** | When acquiring new software, ensure that it’s free from known vulnerabilities and apply patches where necessary. |
| **Manage access control policies & IT assets** | Train your employees in security practices, manage access rights to systems, and monitor the use of IT assets. |
| **Install secure communication tools & emergency communication systems** | Install secure communications, and resources to coordinate responses in the event of a major incident, e.g., a crisis room equipped with reliable communications technology. |
| **Plan for incident handling** | Produce a cyber-attack response plan, including notification of incidents to the appropriate authorities. |
| **Prepare your risk analysis** | Define procedures to assess the vulnerabilities of your information systems and draw up a security policy (including supply chain security) to mitigate these risks. |
| **Outline your business continuity & recovery plan** | Draw up a business continuity plan to guarantee the availability of your services in the event of a disruption, such as a server failure. |
| **Define cryptography policies** | Define policies on the use of cryptography to protect sensitive data, for example, by encrypting sensitive communications. |
| **Assess cyber risk management measures ongoing** | Regularly reassess your security setup through audits and vulnerability tests. |

# How will medical device manufacturers be impacted?

**Complying with the NIS 2 Directive | International standards**

**The NIS 2 Directive regulations reference that companies should consider compliance with international standards**.

### Benefits of ISO 27001 certification

Attaining ISO 27001 certification for information security management systems is a logical first step. An ISO 27001-compliant ISMS enables an organisation to reduce its risk and exposure to security threats by identifying:

- The relevant policies that need to be documented
- The technologies required to protect itself
- The staff training necessary to avoid issues

It also mandates that the organisation conducts annual risk assessments, which proactively anticipate the evolving risk landscape, and facilitates independently audited certification which provides evidence to suppliers, stakeholders, and regulators that you've taken the appropriate and proportionate technical and organisational measures required.

### Benefits of ISO 22301 certification

A further measure to demonstrate compliance with NIS 2 involves ISO 22301 certification. ISO 22301 is structured to help organisations implement, maintain, and continuously improve their approach to business continuity. Whilst ISO 27001 includes business continuity management (BCM), it doesn't define a specific process for implementation. As such, ISO 22301 complements ISO 27001 with its inclusion of this process.

The combination of **ISO 27001** and **ISO 22301** certification enables the creation of a compliant and effective integrated management system comprising both an ISMS and a BCMS – facilitating continuous limitation of risk and exposure to security threats.

**Tip | Guidance issued by the European Union Agency for Cybersecurity (ENISA) maps security objectives to several best practice standards.**

## What does this mean for Swiss legislation?

The Information Security Act (ISG) entered into force on 1 January this year. This decision from the Swiss Federal Council marks an important milestone in protecting information and strengthening cybersecurity in Switzerland.

The ISG, which combines the most important legal bases for the security of federal information and IT resources, prescribes uniform minimum requirements for federal authorities and organisations based on international standards. It also extends the scope of protection to third parties, cantons, and international partners entrusted with the processing of sensitive federal data.

It's worth noting, that the ISG does not specifically apply to medical device manufacturers. As such, medical device companies should refer to NIS-2 to comprehensively fulfil cybersecurity requirements from a business perspective - especially when dealing with companies in the EU market.

Congenius

**Should you have a cybersecurity challenge, please do get in touch – our eHealth team is ready and happy to help.**

For more regarding cybersecurity for medical devices, see this Congenius whitepaper.

And for the full series of articles on the latest horizontal directives & regulations, see here.

Congenius AG
Riedstrasse 1
CH - 8953 Dietikon

E: info@congenius.ch
T: +41 44 741 04 04

congenius.ch

Revision 1 – August 2024