

# NIS2 Consulting Service

## Cyber Security Directive (NIS2)

Requires that the entities implement appropriate and proportionate technical, operational and organisational measures:

- **To manage the risks** of the security of the network and information systems they use in their operations or services.
- **To prevent or minimize the impact of deviations** on the recipients of their services.

Entities are divided into critical sectors and other critical sectors.

**The new** Cybersecurity Directive (NIS2) that has come into force has brought new obligations on organisations' digital risk management.

These include, among others:

- 1) cyber risk management implementation and monitoring
- 2) registering on the operator list,
- 3) arranging cyber training for every level of staff,
- 4) identifying suppliers in the supply chain, and
- 5) reporting incidents.

## WE SUPPORT COMPANIES IN IMPLEMENTING THE NEW LEGISLATION.

### We provide assistance with:

- 1) Organising training:
  - NIS2 implementation training (2 hrs)
  - Cyber situational awareness for the personnel (once / month, 1 hrs)
  - Training modules 1–10, (3 hrs / module)
  - MIF: Cyber Master Basics & Cyber Master Extended (3 day + 2 day)
  - Other Cyberwatch's lectures and online courses
- 2) Defining and registering your entity:
  - Does NIS2 concern the entity
  - Critical sector or other important sector
- 3) Cyber risks consultation and in creating a risk management process
- 4) Checking the security of the supply chain
- 5) Other NIS2-related questions

**We offer a free introduction to the requirements of the Cybersecurity Act!**



Cyberwatch Oy | +358 40 500 8177  
info@cyberwatchfinland.fi

