CHOOSING THE RIGHT CYBER FUNDAMENTALS ASSURANCE LEVEL FOR YOUR ORGANIZATION – healthcare sector

This tool is developed by the Centre for Cybersecurity Belgium to conduct an easy risk assessment resulting in a well-informed selection of the appropriate Cyber Fundamentals Assurance Level in the context of NIS2.

Healthcare sector	Healthcare providers; EU reference laboratories; R&D of medicinal products; manufacturing basic pharma products and preparations; manufacturing of medical devices critical during public health emergency
	Special case: entities holding a distribution authorization for medicinal products: **only** if identified as CER

Healthcare — CyFun Risk Assessment Summary

Organization Size (L/M/S = 3/2/1): 3
Total Risk Score: 217.5
CyFun Level: ESSENTIAL

Threat Actor Types

Competitors — Ideologues / Hactivists — Terrorists — Cyber Criminals — Nation State Actors

Cyber Attack Categories and Risk Details

1. Sabotage / Disruption (DDOS, …)

- Global or Targeted: 2
- Impact: High
- Competitors: Low (0)
- Ideologues / Hactivists: Medium (30)
- Terrorists: Medium (30)
- Cyber Criminals: Low (0)
- Nation State Actor: Medium (30)

2. Information Theft (espionage, …)

- Global or Targeted: 2
- Impact: High
- Competitors: Low (0)
- Ideologues / Hactivists: Low (0)

- Terrorists: Medium (30)
- Cyber Criminals: Medium (30)
- Nation State Actor: Medium (30)

3. Crime (Ransom attacks)

- Global or Targeted: 1
- Impact: High
- Competitors: Low (0)
- Ideologues / Hactivists: Low (0)
- Terrorists: Low (0)
- Cyber Criminals: High (30)
- Nation State Actor: Low (0)

4. Hactivism (Subversion, defacement…)

- Global or Targeted: 1
- Impact: Low
- Competitors: Low (0)
- Ideologues / Hactivists: Low (0)
- Terrorists: Low (0)
- Cyber Criminals: Low (0)
- Nation State Actor: Low (0)

5. Disinformation (political influencing)

- Global or Targeted: 1
- Impact: Medium
- Competitors: Low (0)
- Ideologues / Hactivists: Medium (7.5)
- Terrorists: Low (0)
- Cyber Criminals: Low (0)
- Nation State Actor: Low (0)

Summary of Risk Scores

- Competitors: 0
- Ideologues / Hactivists: 37.5
- Terrorists: 60
- Cyber Criminals: 60
- Nation State Actor: 60

Probability

- **Low (0):**
  This type of threat actor is not known to have executed this kind of attack in this sector.
  There are no indications that this might be the case in the near future.
  Risk evaluation: Risk is acceptable as is — the risk can be accepted without further action.
- **Medium (0.5):**
  This type of threat actor is known to have executed this kind of attack globally.
  It is reasonable to accept that this might be the case in this sector in the near future.
  Risk evaluation: Risk is tolerable under control — a follow-up in terms of risk management shall be conducted and actions shall be set up in the context of medium- and long-term continuous improvement.
- **High (1):**
  This type of threat actor is known to have executed this kind of attack in this sector.
  It is reasonable to assume that this will reoccur in this sector in the near future.
  Risk evaluation: Risk is unacceptable — measures for reducing the risk shall absolutely be taken in the short term. Otherwise, all or a portion of the activity should be discontinued.

Impact

- Low = 0
- Medium = 5
- High = 10

CyFun Level

- 0–99 → BASIC
- 100–199 → IMPORTANT
- 200–10,000 → ESSENTIAL

Type of Attack and Required Protection Value

- **Global:** 1
- **Targeted:** 2

In global or un-targeted attacks (value 1), attackers indiscriminately target as many devices, services, or users as possible.
They do not care about who the victim is, as there will be a number of machines or services with vulnerabilities.

Targeted attacks refer to a type of threat in which threat actors actively pursue and compromise a target entity’s infrastructure.
Typically, these threat actors have a certain level of expertise and have sufficient resources to

conduct their schemes over a long-term period.

For this reason, a greater degree of protection is required (value 2).