



This is your Cyber Score. The score is a number between 1 and 10. The higher the score, the better your cybersecurity is according to the NIS2 standards.

What does your NIS2 Cyber Score mean?

Explanation per NIS2 Cyber Score (1 to 10)

Below you'll find a detailed explanation of what your score means, why it matters, and how to respond to it wisely. This explanation is intended to help companies reflect, not to judge. Think of it as a roadmap towards digital resilience.



Score 8.5 – 10: Excellent – your cybersecurity is well organised

Your organisation is secure and professionally managed.

Why is this important? Digital security is not just about compliance; it's about trust. You are now able to take on assignments where security is a prerequisite. You strengthen your market position and reduce your liability.

Are you ready? Absolutely, if you have achieved the NIS2 Quality Mark and passed the audit. Now you just need to maintain everything properly. Use your score and the NIS2 QM certificate actively in your communication with clients.

If you only have ISO27001, check whether the gap has been closed. There is a gap between NIS2 legislation and ISO27001. Familiarise yourself with this if you do not yet have NIS2 QM certification. This way, you can strive for 100% NIS2 compliance.

Share your story with other companies – this helps build a stronger supply chain.

Samen Digitaal Veilig can help raise your cybersecurity to the next level. Often it's not about doing more work, but about organising things more smartly. The platform is an initiative of more than 100 industry associations and knowledge partners. The goal is to help all companies in the chain comply with NIS2 – without doing too much or incurring excessive costs.

Check your NIS2 Cyber Score

Organisation

2. Does your organisation have a cybersecurity plan (Information Security Policy)?

1 2 3 4 5 6 7 8 9

3. Has the management signed this plan?

No

Unknown

4. How well is your organisation protected against the impact on your customers in the event of a cyber attack?

1 2 3 4 5 6 7 8 9

5. Do you (or does your organisation) have access to customers' systems or data?

No

Unknown

6. How well do you secure access to your customers' systems or data?

1 2 3 4 5 6 7 8 10

7. How well is access to customer data or systems secured within your organisation?

1 2 3 4 5 6 7 8 10

8. Do you have a plan to respond quickly to a cyber incident?

No

Unknown

9. Has your company obtained any cyber certification such as NIS2QM, ISO27001, or another standard?

No

Unknown

10. If certified: which certification does your company have?

• NIS2 QM

• NEN7510

• Not applicable

• Other, namely: (please specify)

Employees

11. How many employees does your company have?

1-3

3-10

10-25

25-100

100-250

250-1000

>1000

12. To what extent are employees trained in cyber security?

1

2

3

4

5

6

7

8

9

10

13. How do employees within your organisation handle software updates?

1

2

3

4

5

6

7

8

9

10

14. Is there a team/member appointed who is responsible for the cybersecurity plan and its continuation?

Yes

No

Unknown

15. Are all employees within your company familiar with the contents of the cybersecurity plan?

1

2

3

4

5

6

7

8

9

10

Technology

16. Are regular backups made of important systems and data within your organisation?

Yes

No

Unknown

17. Does your organisation have a plan for creating and restoring backups of important data, and have you tested this in the past year?

1

2

3

4

5

6

7

8

9

10

18. Do you have a list of which data and systems must always be backed up?

Yes

No

Unknown

19. Are new important systems or software automatically included in your organisation's backup schedule?

No

Unknown

20. Have you taken measures to protect the company against viruses and other malware?

1

2

3

4

5

6

7

8

10

21. Has there ever been an external inspection or internal audit conducted to check your security?

No

Unknown

22. Have you taken measures to prevent malicious actors from taking over your email accounts?

1

2

3

4

5

6

7

8

9

23. Do you regularly review who has access to your (IT) systems and remove access for former employees and external parties?

1

2

3

4

5

6

7

8

9

24. Are there rules about who is allowed physical access to computers, servers, and other sensitive areas?

No

Unknown

Suppliers

25. Do you know which external suppliers pose a risk?

1

2

3

4

5

6

7

8

9

26. Do you know the impact on your company for each supplier if they are affected by a cyber incident and can no longer deliver?

No

Unknown

27. Have you made agreements with external suppliers who pose a risk to you?

No

Unknown

28. Have you communicated with your suppliers about the importance of secure (cyber) practices, and have clear agreements been made?

No

Unknown

29. Have you agreed with your suppliers that they will report any cybercrime incidents that could affect your organisation?

No

Unknown

30. Have you asked your suppliers if they hold a security certification, such as ISO 27001, the NIS2 Quality Mark, or another standard?

No

Unknown

31. Do you have an understanding of the impact on your customers if a supplier can no longer deliver?

1

2

3

4

5

6

7

8

9

32. Do you know how long your organisation can operate without the products and/or services of your key suppliers without disrupting business operations?

1

2

3

4

5

6

7

8

9

33. Do you understand the damage that could occur if business information and/or business plans become public through external parties?

1

2

3

4

5

6

7

8

9

34. Do you know to what extent key parts of your organisation depend on specific ICT services, systems, or products from suppliers?

1

2

3

4

5

6

8

9

10

35. Are supplier employees allowed access to locations where sensitive information, IT equipment, or information systems are present?

Yes

Unknown